[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04K 1/00
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 99807072.6

[43]公开日 2001年7月18日

[11]公开号 CN 1304602A

[22]申请日 1999.5.5 [21]申请号 99807072.6
[30]优先权
[32]1998.5.5 [33]US [31]60/084,257
[86]国际申请 PCT/US99/09938 1999.5.5
[87]国际公布 WO99/57835 英 1999.11.11
[85]进入国家阶段日期 2000.12.5
[71]申请人 杰伊·C·陈
地址 美国加利福尼亚州
[72]发明人 杰伊·C·陈

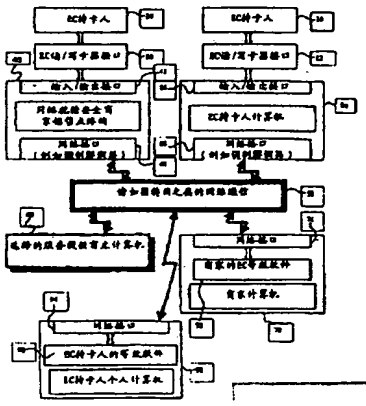
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李德山

权利要求书9页 说明书33页 附图页数29页

[54]发明名称 一种用于电子交易的密码系统和方法

[57]摘要

一种电子交易系统，该系统简化了包括持卡人(20)，商家(70)和服务提供商(SP)(60)的多个交易方之间的安全电子交易。该系统涉及通常被称为智能卡的电子卡，以及它们的等效计算机软件包。电子卡模仿真实的钱包，并含有诸如信用卡、支票簿或驾驶执照之类的常见金融或非金融载具。交易受到混合密钥加密系统的保护，并且通常在诸如因特网之类的公共网络上执行。数字签名和随机数被用于确保完整性和真实性。电子卡使用诸如由服务提供商(SP)分配的对话密钥之类的保密密钥，确保每项交易的保密性。SP独自负责验证每个交易参加者的敏感消息，并分配对话密钥。交易中所需的唯一信任关系是单个交易参加者和SP之间所存在的那种信任关系。



ISSN1008-4274

权　利　要　求　书

1. 一种用于电子交易的系统，包括:

电子卡，它具有

用于加密和解密的密码服务，

存储信息的数据区，和

存储持卡人和服务提供商会员终端的数据区;

响应电子卡的服务提供商会员终端；和

与服务提供商信息通信的服务提供商终端。

2. 按照权利要求 1 所述的系统，其中电子卡是实际的卡。

3. 按照权利要求 1 所述的系统，具有该电子卡功能的软件。

4. 按照权利要求 1 所述的系统，其中电子卡还包括用于载入和更新持卡人信息，改变 PIN，以及管理服务提供商数据区的卡操作系统。

5. 按照权利要求 1 所述的系统，其中电子卡执行外部通信读/写操作，以及通信协议处置。

6. 按照权利要求 1 所述的系统，其中电子卡还包括管理电子卡的软件。

7. 按照权利要求 1 所述的系统，其中用于存储服务提供商信息的数据区包括服务提供商记录，服务提供商记录包括:

指示服务提供商的名称字段;

密钥值；和

含有每个服务提供商独有的信息的帐户信息字段。

8. 按照权利要求 1 所述的系统，其中电子卡还包括应用软件。

9. 按照权利要求 1 所述的系统，还包括小应用程序　程序。

10. 按照权利要求 1 所述的系统，还包括外部系统，其中服务提供商终端与外部系统通信。

11. 按照权利要求 7 所述的系统，其中每个服务提供商记录还包括规定服务提供商支持的载具（instrument）种类的卡类型字段。

12. 一种使用电子卡执行电子交易的方法，该方法包括下述步骤:

在服务提供商处产生对话密钥;

通过从会员向服务提供商发送密钥，并从服务提供商向该会员发送对话密钥，交换密钥；和

利用该对话密钥执行交易。

13. 按照权利要求 12 所述的方法，其中交易密钥的步骤包括下述步骤:

从会员向服务提供商发送密钥交易请求消息；和

格式化包括发给会员的对话密钥的密钥交换响应，并把该密钥交换响应发送给会员。

14. 按照权利要求 12 所述的方法，其中利用对话密钥执行交易的步骤包括下述步骤:

利用对话密钥格式化会员交易请求消息，并把会员交易请求消息发送给服务提供商；和

在服务提供商处，格式化要发给会员的交易响应消息，并把该交易响应消息发送给该会员。

15. 按照权利要求 12 所述的方法，其中使用对话密钥执行交易的步骤包括下述步骤:

第一会员利用对话密钥格式化交易请求消息，并把交易请求消息发送给第二会员，交易请求消息包括第一会员的数字签名；和

第二会员利用对话密钥格式化交易响应消息，并把交易响应消息发送给第一会员，交易响应消息包括第二会员的数字签名。

16. 按照权利要求 12 所述的方法，其中利用对话密钥执行交易的步骤包括下述步骤:

第一会员利用对话密钥格式化交易请求消息，并把交易请求消息发送给中间会员，交易请求消息包括第一会员的数字签名;

中间会员利用对话密钥格式化交易响应消息，并把交易响应消息发送给最后的会员，交易响应消息包括中间会员的数字签名;

最后的会员利用对话密钥格式化交易响应消息，并把交易响应消息发送给第一会员，交易响应消息包括最后的会员的数字签名。

息；

如果第一方是交易参加者，则组合第一方的密钥交换请求消息和电子卡的密钥交换请求消息，并把组合的密钥交换请求消息发送给下一方；

如果当前一方是消息路由器，则把密钥交换请求消息发送给下一方；

如果当前一方是交易参加者，则组合当前一方的密钥交换请求消息和上一方的密钥交换请求消息，并把组合的密钥交换请求消息发送给下一方；

由服务提供商把发给每个交易参加者的密钥交换响应格式化成一个消息，并沿着把密钥交换请求消息发送给服务提供商的路径的相反顺序，发送该消息；

每个交易参加者使发给它自己的密钥交换响应和发给其它交易参加者的密钥交换响应分开，并沿着把密钥交换请求消息发送给服务提供商的路径的相反顺序，把剩余的密钥交换响应转发给其它交易参加者，直到电子卡收到它自己的密钥交换响应为止。

39. 一种在串联排列的多个交易方之间执行电子交易的方法，包括下述步骤：

从电子卡向第一方发送交易请求消息，这里第一方是消息路由器或交易参加者；

如果第一方是路由器，则从第一方向下一方发送交易请求消息；

如果第一方是交易参加者，则组合第一方的交易请求消息和电子卡的交易请求消息，并把组合的交易请求消息发送给下一方；

如果当前一方是消息路由器，则把交易请求消息发送给下一方；

如果当前一方是交易参加者，则组合当前一方的交易请求消息和上一方的交易请求消息，并把组合的交易请求消息发送给下一方；

由服务提供商把发给每个交易参加者的交易响应格式化成一个消息，并沿着把交易请求消息发送给服务提供商的路径的相反顺序，发送该消息；

每个交易参加者使发给它自己的交易响应和发给其它交易参加者的交易响应分开，并沿着把交易请求消息发送给服务提供商的路径的相反顺序，把剩余的交易响应转发给其它交易参加者，直到电子卡收到它自己的交易响应为止。

40. 一种在被安排成层次组织的多个交易方之间执行电子交易的方法，包括下述步骤:

从电子卡向第一方发送密钥交换请求消息，这里第一方是消息路由器或交易参加者;

如果第一方是消息路由器，则把密钥交换请求消息发送给下一方 $X_{j,k}$（j=2，3，4，…；k=1，2，3，…，m；m 是类型 n 的变量；n=1，2，3…；对于不同的 j 值来说，m 可是不同的值）;

如果第一方是交易参加者，则组合第一方的密钥交换请求消息和电子卡的密钥交换请求消息，并把组合的密钥交换请求消息发送给下一方 $X_{j,k}$;

如果当前一方 $X_{j,k}$ 是消息路由器，则把密钥交换请求消息发送给下一方 $X_{j,k}$;

如果当前一方 $X_{j,k}$ 是交易参加者，则组合当前一方 $X_{j,k}$ 的密钥交换请求消息和上一方的密钥交换请求消息，并把组合的密钥交换请求消息发送给下一方 $X_{j,k}$;

由服务提供商把发给每个交易参加者的密钥交换响应格式化成一个消息，并沿着把密钥交换请求消息发送给服务提供商的路径的相反顺序，发送该消息;

每个交易参加者使发给它自己的密钥交换响应和发给其它交易参加者的密钥交换响应分开，并沿着把密钥交换请求消息发送给服务提供商的路径的相反顺序，把剩余的密钥交换响应转发给其它交易参加者，直到电子卡收到它自己的密钥交换响应为止。

41. 一种在被安排成层次组织的多个交易方之间执行电子交易的方法，包括下述步骤:

从电子卡向第一方发送交易请求消息，这里第一方是消息路由器

或交易参加者;

如果第一方是消息路由器，则把交易请求消息发送给下一方 $X_{j,k}$（j=2，3，4，…；k=1，2，3，…，m；m 是类型 n 的变量；n=1，2，3…；对于不同的 j 值来说，m 可是不同的值）;

如果第一方是交易参加者，则组合第一方的交易请求消息和电子卡的交易请求消息，并把组合的交易请求消息发送给下一方 $X_{j,k}$;

如果当前一方 $X_{j,k}$ 是消息路由器，则把交易请求消息发送给下一方 $X_{j,k}$;

如果当前一方 $X_{j,k}$ 是交易参加者，则组合当前一方 $X_{j,k}$ 的交易请求消息和上一方的交易请求消息，并把组合的交易请求消息发送给下一方 $X_{j,k}$;

由服务提供商把发给每个交易参加者的密钥交换响应格式化成一个消息，并沿着把密钥交换请求消息发送给服务提供商的路径的相反顺序，发送该消息;

每个交易参加者使发给它自己的交易响应和发给其它交易参加者的交易响应分开，并沿着把交易请求消息发送给服务提供商的路径的相反顺序，把剩余的交易响应转发给其它交易参加者，直到电子卡收到它自己的交易响应为止。

说　　明　　书

一种用于电子交易的密码系统和方法

本发明涉及用于安全电子交易的密码系统和方法，更具体地说，涉及一种电子卡，该电子卡采取“智能卡”和/或其等效软件的形式。

通称“智能卡”一般表示集成电路（IC）卡，即，嵌有微芯片的信用卡大小的塑料片。智能卡上的IC芯片通常，但不是必须地，由微处理器（CPU），只读存储器（ROM），随机存取存储器（RAM），输入/输出装置，和诸如电可擦可编程只读存储器（EEPROM）之类的一些持久性存储器组成。该芯片能实现算术计算，逻辑处理，数据管理以及数据通信。

智能卡主要分成接触式和非接触式两种。国际标准组织（ISO）已在ISO系列下制定了关于这种电子卡的规范。特别地，ISO 7816适用于集成电路卡。由于其具有计算能力，智能卡可支持许多安全特征，例如认证，安全读/写，对称性密钥和非对称性密钥加密/解密。这些智能卡安全特征使智能卡非常适合于电子商务，在电子商务中，数据安全和认证是最重要的。

智能卡已被应用于许多特定领域中，例如公共交通，健康保险，停车场，校园，加油站等等。并且其在电子商务和其它金融领域中的潜在应用，正在以较快的步伐日益普及。在1996年5月28日授予Robert S. Power的美国专利No.5521362，“具有多个存储器以防止欺诈使用的电子钱包及其方法”描述了一种电子钱包应用。Power的发明证明了智能卡被用作安全的金融工具的能力，而不仅仅是用作存储装置。

随着技术的进步，使智能卡芯片的计算速度越来越快，存储器容量越来越大，“多用途智能卡”的概念日益变得从经济上和物理上均是可行的。1996年6月25授予Douglas C. Tarylor的美国专利No.5530232，“多用途数据卡”描述了一种多用途卡，该多用途卡能够代替各种现有的单用途卡，并能满足金融和非金融要求。该多用途卡

使用常规的数据链路连接智能卡和远程服务提供商。Taylor 的多用途卡专利并不涉及任意类型的开放式网络或加密方法。

1996年8月5日授予Mandelhaum等的美国专利No.5544246，“适于多个服务提供商，并且适于其远程设置的智能卡”描述了一种智能卡，该智能卡允许不同的服务提供商共存于同一智能卡上。每个服务提供商被看作是智能卡的一个用户，并由智能卡的发行者/所有者设置在该智能卡上。允许每个用户建立树形文件结构，并利用口令文件保护其树形文件结构。Mandelbaum 的发明描述了一种允许产生和删除多种应用的智能卡。Mandelbaum 的智能卡通过使用适当的口令文件控制对每种应用的访问。

1997年9月23日授予Taher Elgamal的美国专利No.5671279，“使用安全信使系统的电子商务”描述了一种利用公钥/密钥密码学，在公用网络上实现电子商务的系统。Elgamal 的专利没有提及智能卡作为实施电子商务的工具的应用，并且是通过利用数字凭证来验证电子商务参与者的。安全信使系统需要诸如因特网之类开放式网络上，交易各方之间的安全通道，例如安全套接层（Secure Socket Layer）（SSL）。

1998年8月4日授予Fox等的美国专利No.5790677，“用于安全电子商务交易的系统和方法”描述了具有位于交易程序之前的登记程序的系统和方法。在登记阶段中，每一位交易参与者通过向服务器发送登记包，登录信任的凭证约束服务器（trusted credential binding server）。服务器根据接收的请求，产生独特的凭证，并将其发送给请求发起者。在交易阶段中，交易的发起者请求，接收并核实商务文件和/或契约的所有预期接受者的凭证，并利用单独接受者的公钥对文件和/或契约加密。这样，各个接收方可解密并访问只打算供其使用的商务文件。Fox 的专利描述了反映所谓的“安全电子交易”（SET）标准的主题的程序，安全电子交易标准是由几家主要的金融公司和软件公司目前正在共同支持的一项计划，以便建立基于电子商务系统的数字凭证和凭证管理机构。

1998年8月18日授予Derek L. Davis的美国专利No.5796840，“提供保密通信的设备和方法”描述了一种半导体器件，该半导体器件能够产生将在后续的消息验证和数据通信中使用的特定于器件的密钥对。该半导体器件使用公钥/密钥密码学，以确保通信双方的可靠性。

1996年7月9日授予Simon G. Laing和Matthew P. Bowcock的美国专利No.5534857，“实现智能卡的安全，分散个人化的方法和设备”描述了把来自发行者的机密数据安全地写入位于远方的用户智能卡的方法和设备。通过使用存储在保密计算机和零售商智能卡中的公用密钥，产生用于对保密终端和保密计算机之间的数据传送进行加密的共同对话密钥。

根据上面提及的发明，显然安全电子商务系统的结构涉及公钥基础结构和与之相关的数字凭证管理机构。

开放式网络中，基于保密密钥的系统在密钥分配和密钥管理方面灵活性较差。另一方面，基于公钥/密钥的系统固然有优于保密密钥系统的优点，但是也具有自己的使人望而生畏的任务，即使交易各方相互认证。本发明提出另一种系统和方法，该系统和方法不需要凭证管理机构和数字凭证。本发明是一种用于电子交易的混合系统。该混合系统在密钥交换阶段内使用公钥/密钥，并在交易阶段中使用对话密钥作为保密密钥。

本发明是用于使用电子卡（EC）并通过通信网络联系的电子交易的密码系统和方法，该电子卡呈智能卡或等效软件的形式。

本发明的优选实施例使用开放式网络，例如因特网。本发明的备选实施例可使用其它类型的网络。本发明的一个实施例或者使用物理的智能卡，或者使用实现为计算机软件包，并在诸如个人计算机（PC）之类的计算装置上运行的智能卡。同样，交易中涉及的商家可使用作为销售点终端的商家装置，或者使用主计算机上的软件与EC和服务提供商通信的装置。当使用智能卡时，需要智能卡读卡器，以允许智能卡与主设备，例如网络就绪商家终端，PC或者能够支持智能卡交易的任意其它电子装置通信。

在基于公共密钥和数字凭证的系统中，交易参加者通过利用由凭证管理机构（CA）或证书约束服务器签发和证明的数字凭证或其它电子证书，交换公共信息。CA 或服务器与每个交易参加者之间的通信必须保密。随机数和数字签名被用于确保在交易参加者之间传送的消息的真实性和有效性。

本发明的优选实施例的密码系统和方法也使用公共/专用密钥密码法，不过运用方式稍有不同。本发明的密码系统和方法并不试图建立另一种信任关系，这种信任关系类似于存在于数字凭证持有者和凭证管理机构之间的那种信任关系。本发明特别地是以大型的会员制金融机构，诸如大型的信用卡公司及其所有持卡人，或者主要银行和其所有 ATM 持卡人作为其潜在用户。非金融机构也可使用这种密码系统和方法，从而通过网络执行电子商务或非金融交易。

服务提供商（SP）向其会员提供某些服务。金融机构正是一种类型的服务提供商。服务提供商在本质上还可以是非金融的。不论服务提供商是金融机构还是非金融机构，产生的过程基本相同。涉及金融机构的交易和涉及非金融机构的交易之间的唯一区别是消息可能包括不同的数据字段。

当 EC 持卡人和服务提供商之一签订使用服务契约之后，服务提供商在 EC 上产生一个专用表目。每个表目含有服务提供商的帐户信息，SP 的公共密钥，存取控制信息和其它相关数据。每个 EC 可支持预定数目（例如 10）的这种表目，并且每个这种表目代表一个服务提供商。

通过使用公共/专用密钥密码学，极大地简化了密钥分配过程。EC 持卡人他/她自己或者任意受托第三方，例如银行支行或者甚至邮局都可执行密钥分配工作。SP 的公共密钥只用于 SP 和持卡人之间的初始密钥交换。在初始密钥交换步骤之后，SP 分配对话密钥，对话密钥保护持卡人和 SP 之间，或者持卡人他们自己之间的任意进一步消息交换。

这种既使用公共密钥/专用密钥密码学又使用保密密钥密码学（即

对话密钥）的混合系统和其它保密密钥系统的不同之处在于：在混合系统中，保密密钥（即对话密钥）只对单个对话期有效，不适用于其它对话期。对话期具有确定的时间长度。当超逾时间期限或者当条件被满足时，对话期会终止。

在交易中涉及商家的情况下，商家经历大体和 EC 持卡人相同的程序和 SP 通信。商家将首先执行与 SP 的密钥交换，并接收对话密钥。对话密钥将由商家用于与 SP 的后续通信。持卡人和商家对发给 SP 的每条消息进行数字签名，SP 类似地对回送给持卡人和商家的响应消息签名。

在交易需要与另一基于以电子凭证为交易机制的系统的相互作用的情况下，在基于在初始的密钥交换之后的进一步信息交换，验证持卡人和商家之后，SP 可充当持卡人和商家的凭证代理人。在最极端的情况下，SP 独立地执行该代理功能，变成以电子凭证为交易机制的系统的网关。这种类型的层次结构是非常理想的，因为减少了在多个系统之间，执行交易所需的信任关系的数目。另外，用户因此不必携带凭证。

图 1 是表示根据本发明的一个实施例的系统的各个部分之间的系统的方框图。

图 2 表示了经过网络的这两个交易阶段的流程。

图 3 是 EC 的概略表示。

图 4 表示了服务提供商数据区的格式。每个服务提供商的信息在该表中被分配一个表目，并受到存取条件的保护。

图 5 表示了数字签名是如何用在本发明的实施例中的。

图 6A-6Q 表示了为了通过开放式通信网络，例如因特网，执行电子交易，在本发明的一个实施例中使用的密码系统和方法的示意流程图。

图 7-11 描绘了在密钥阶段和交易阶段中，组合请求和响应消息的最终格式和内容。

图 12 表示了一个服务提供商与被串联布置的多个交易参加者进行

交易。

图 13 表示了一个服务提供商在网络上与已被布置成层次组织形式的多个交易参加者进行交易。

本发明的优选实施例是一种利用呈智能卡或等效软件形式的电子卡（EC），并通过通信网络通信的，用于电子交易的密码系统和方法。

在本发明优选实施例中，网络是诸如因特网之类的开放式网络。在本发明的备选实施例中，可使用其它开放式网络和/或封闭式网络建立服务提供商和其会员之间的通信。例如，服务提供商可使用其自己所有的金融网络和其会员通信。

任何因特网协议可用于因特网连接。可使用的协议的例子包括 TCP/IP，UDP，HTTP 等等。

也可借助诸如使用传统的模拟电话业务（又名简易老式电话业务或 POTS）的公用交换电话网络（PSTN）之类的通信网络传送业务，或者通过使用诸如 T-1，E1 或 DS-3 数据电路，综合业务数字网络（ISDN），数字用户线路（DSL）业务之类的数字通信业务，或者甚至使用无线业务等等，实现通信。当利用这种业务实现时，可独立于通信协议（即，在电子接口层）实现本发明。

还可借助局域网（LAN）或广域网（WAN），例如以太网，令牌网，FDDI，ATM 等等实现通信。可使用的协议的例子包括 TCP/IP，IPX，OSI 等等。

其它通信链路可包括光纤连接，无线 RF 调制解调器连接，蜂窝调制解调器连接，卫星连接等等。

只要在服务提供商和其会员之间可建立通信路径，即可采用本发明。上面的例子是用来举例说明可实践本发明的各种通信环境的几个例子。本领域的普通技术人员清楚，本发明并不局限于上面详述的那些环境。

EC 可采取智能卡或在诸如个人计算机（PC）之类计算机系统上运行的软件包的形式。当 EC 被实现为智能卡时，它可用在诸如 PC 之类的网络就绪（network-ready）计算机系统上，以便和另一会员和

之间的关系的方框图，它涉及一个持卡人，一个商家及一个服务提供商。

EC 持卡人 20 可以经由网络 50 实施交易，并且或者通过利用连接在发端计算机 84 上的 EC 读/写装置 82，或者通过利用在发端计算机 90 运行的 EC 等效软件 92 和商家通信。

商家可通过利用网络就绪的销售点（POS）终端 40，或者通过利用在商家装置 70 上运行的 EC 等效软件，经过网络实施交易，从而经过诸如因特网之类的网络 50 与选定的服务提供商 60 执行电子交易。

一旦对 EC 卡的访问条件被满足，则持卡人可通过网络 50 执行与系统的其它参加者的金融或非金融交易。图 1 中表示了可通过网络执行交易的三种不同方案。

（1）在 POS 交易中（图 1 的左上方），持卡人 20 在商家店铺内将 EC 刷过/插入商家的 EC 读/写卡器 30. EC 读/写卡器与网络就绪的商家 POS 终端 40 相连。网络就绪商家 PSO 终端 40 是一个防止篡改的可编程装置，它包括诸如键盘之类的输入装置，显示器，处理器和 EC 读/写卡器 30（EC 接口装置）. POS 终端 40 通常是一个小型计算机，例如装有与开放式网络的通信链路的 PC. POS 终端经过网络 50 与 SP 通信。

（2）（图 1 的右侧）持卡人可通过把 EC 20 插入读/写装置 82，执行与系统的其它参加者的交易，读/写装置 82 与为发端计算机的持卡人的个人计算机 84 相连。发端计算机和网络 50 相连，使 EC 能够和商家计算机 70 通信。商家计算机 70 具有使商家能够接收 EC 产生的消息，并产生组合 EC 信息和商家信息的消息的 EC 等效软件 72。随后，组合的消息经过网络被发送给 SP。

（3）（图 1 的下方）持卡人可通过利用用户持卡人的个人计算机 90 上的 EC 等效软件 92，执行与系统的其它参加者的交易。交易开始于发端计算机 90，即，持卡人的个人计算机。持卡人通过网络 50 实施交易，并与商家的计算机 70 通信，商家的计算机 70 再经过网络 50 与 SP 60 通信。

/或选定的服务提供商交易。将需要和计算机系统通信的读/写接口装置，以及连接智能卡持有者和网络的一些应用软件，例如因特网浏览器。如果 EC 是载入计算机系统中的软件包，则不需要读/写接口。本发明关于 EC 的例证实施例作电子钱包（或者虚拟钱包）的作用，该电子钱包的功能和真实钱包的相类似。真实钱包可带有信用卡，借记卡，ATM 卡，保健卡（health provider card），会员卡，现金等等。EC 具有所有上述金融和非金融工具的数字等同物，并能够通过因特网实施安全交易。

服务提供商会员可以是商家和/或 EC 卡持卡人。商家是由服务提供商向其支付交易酬金的会员。会员可以既是商家又是 EC 卡持卡人。商家可参与和其它持卡者的交易，其结果是服务提供商向该商家支付交易酬金。商家还可以是 EC 卡持卡人，并从例如供货商那里购买供应品。

密码系统可包括服务提供商和任意数目的服务提供会员之间的通信。这样，通信可在 EC 和 SP 之间，可在商家和 SP 之间，可在第一 EC，第二 EC 和 SP 之间，可在第一商家，第二商家和 SP 之间，等等。EC 可直接和服务提供商通信，以便查询帐户余额。商家可以只以其自己的名义，而不是以 EC 的名义和服务提供商通信，因为，例如商家希望了解他自己与服务提供商的帐户余额。SP 和其会员之间的通信可遵守 SP 和其会员的任意排列组合。SP 和其会员之间的通信链路的组织可以是连续的和/或分层的。SP 和其会员之间的通信也可借助路由器实现，路由器在 SP 和其会员之间按规定路线发送消息。

加密方法是一个分为两阶段的密钥交换-交易模式。第一个阶段是密钥交换阶段。第二个阶段是交易阶段。在密钥交换阶段中，会员和服务提供商交换密钥。会员把他们的密钥发送给服务提供商，服务提供商使用这些密钥向会员发送对话密钥。对话密钥保护持卡人和 SP 之间的，或者持卡人他们自己之间的其它消息交换。在交易阶段中，SP 可主导交易或者持卡人他们自己可实施交易。

图 1 是表示根据本发明的一个例证实施例的系统的各个构成部分

在本发明的优选实施例中，个人计算机被用于保持 EC 等效软件，而在本发明的备选实施例中，其它电子装置可用于保持 EC 等效软件。

在本发明的优选实施例中，用于使 EC 能够和商家通信的网络和用于使商家能够与 SP 通信的网络相同。在另一实施例中，用于使 EC 能够与商家通信的网络可以不同于用于使商家能够与 SP 通信的网络。在又一实施例中，用于使一个商家能够与 SP 通信的网络可不同于用于使另一商家能够与该 SP 通信的网络。在又一实施例中，用于使 EC 能够与商家通信的网络可不同于用于使另一 EC 能够与另一商家通信的网络。一个实施例可由多样性的网络组成，不同的交易各方借助这些网络通信。

在本发明的优选实施例中，交易被分为两个阶段：密钥交换阶段和交易阶段。图 2 是一个特例，图 2 图解说明了 SP 主导交易阶段的两阶段密钥交换-交易模式。当 SP 主导交易时，交易参加者之间不存在任何敏感性信息的直接交换。

在交易阶段位于持卡人他们自己之间，以及在 SP 主导交易阶段的情况下，密钥交换阶段都是相同的。在交易阶段位于持卡人他们自己之间的情况下，持卡人使用 SP 对话密钥相互通信，并执行交易。

图 2 展示了 SP 主导交易阶段的金融交易。所示的交易涉及三方：EC（交易发起者）102，商家 104 和服务提供商（SP）106。发起方是作为顾客的 EC 持卡人，并由计算机 102 表示。计算机 104 代表商家。计算机 106 代表服务提供商。SP 由 EC 和商家双方选择。

图 2 表示了处理流程从 EC 到商家，再到 SP 的金融交易。加密方法的处理流程并不局限于商家和 EC 持卡人之间的任意特定顺序。图 2 仅仅是从 EC 至商家，再至服务提供商的特定交易的一个例子。处理流程也可从商家至 EC，再到服务提供商。图 2 展示了服务提供商会员（这种情况下，为 EC 持卡人和商家）是如何产生，附加及向服务提供商发送消息的。

图 2 中编号为 1-10 的 10 个箭头表示了在这两个交易阶段中，消息是如何在交易三方之间流动的。步骤 1-4 属于密钥交换阶段，步骤 5-10

属于交易阶段。在图 2 中，商家作为 EC 和 SP 之间的中介。在步骤 1 中，EC 格式化产生密钥交换请求，并把该请求发送给商家。在步骤 2 中，商家组合自己的密钥交换消息和 EC 的密钥交换消息，并把组合的密钥交换消息发送给 SP。在步骤 3 中，SP 格式化产生一个给商家的密钥交换响应，格式化产生一个给 EC 的密钥交换响应，组合这两个密钥交换响应，从而形成组合的密钥交换响应，并把组合的密钥交换响应发送给商家。在步骤 4，商家使发给商家的密钥交换响应和发给 EC 的密钥交换响应分开，并把 EC 的密钥交换响应消息转发回 EC。步骤 4 终结密钥交换阶段中的主要活动。

交易阶段开始于步骤 5。在步骤 5 中，EC 格式化产生其交易请求消息，并把该消息发送给商家。在步骤 6 中，商家组合接收的交易请求消息和它自己的交易请求消息，并把组合的交易请求消息发送给 SP。在步骤 7 中，SP 格式化产生一个给商家的交易响应消息，格式化产生一个给 EC 的交易响应消息，组合这两个交易响应消息，并把组合的交易响应消息发送回商家。在步骤 8 中，商家使发给商家的交易响应消息和发给 EC 的交易响应消息分开，并把 EC 的交易响应消息转发回 EC。在步骤 9 中，EC 格式化产生确认消息，并把确认消息发送给商家。在步骤 10 中，商家组合接收的确认消息和它自己的确认消息，并把组合的确认消息发送给 SP。步骤 10 终结交易的交易阶段。

虽然图 2 展示了一个简单的交易，但是一些交易可能涉及多个消息。在一些交易过程中，为了完成每个阶段，可能需要一个以上的消息，即使是这种情况下，这些消息仍将遵守相同的组合规则和流程模式。例如，在交易阶段中，SP 可能要求 EC 和商家首先发送帐户信息。如果帐户信息被验证为有效的，则 SP 在响应消息中发送帐户信息的确认消息。一旦商家和 EC 接收该响应消息，则 EC 和商家在传送给 SP 的下一消息中发送交易金额和其它与交易相关的信息。SP 随后批准或否决该交易。图 2 中的步骤既适用于帐户消息，又适用于交易消息。

如果交易的完成要求和诸如基于公钥和数字凭证的系统 108 之类的外界系统的的交互作用，则 SP 将起 EC 和商家的凭证代理人的作用，

并以 EC 和商家的名义与外界系统打交道。本发明的一个理想结果是使交易的所有参加者与外界系统隔绝，从而降低完成交易所需的信任关系的数目。如果交易的一个参加者具有本系统和外界系统的双重会员身份，则他可以选择充当本系统的会员或者充当外界系统的会员。在后一情况下，SP 将利用外界系统的规则面接该参加者。例如，为了和基于公钥和数字凭证或证书的外界系统打交道，SP 在其所有物中具有满足外界系统要求的信任关系的全部所需凭证或证书。为了 SP 和外界系统完成由 EC 和商家发起的交易，需要这样的凭证。这种情况下，只有 SP 需要具有与外界系统的信任关系。基于这种信任关系，单个的 EC 和商家能够和假定的外界系统完成交易。

图 3 表示了 EC 的一个优选实施例。在本发明的一个优选实施例中，EC 在内部由图 3 中所示的软件/硬件部分构成。EC 基于 ISO 7816 标准，并支持 ISO 7816 中规定的同类型的通信协议和命令。

EC 具有管理 EC 内部资源的卡操作系统 550。卡上的加密装置 650 可以软件的形式实现，或者由加密协处理器（图 3 中未表示），或者其它硬件解决方案，或者软件和硬件混合物实现。

EC 的一个独有特征是 EC 存储器中的服务提供商数据区（SPDA），该数据区含有服务提供商的帐户和密钥信息。服务提供商数据区（SPDA）700 含有许多存储槽。在优选实施例中，SPDA 含有预定确定数目（例如 10 个）的存储槽—每个存储槽用于一个可能的服务提供商。在另一实施例中，存储槽的数目是可动态改变的。关于每个服务提供商的记录可被放入一个空的存储槽中。每个记录含有特定服务提供商的帐号、公钥、以及其它相关信息。

根据 EC 设计，SPDA 可选择性地允许每个 SP 包括一些管理其自己的卡上数据，并提供 SP 卡数据和主应用程序之间的接口的软件（例如 JAVA 术语中的“小应用程序”）。换句话说，SPDA 不仅可含有简单的数据；SPDA 可允许每个 SP 把自有的应用程序（例如小应用程序）放到 EC 上，以便向持卡人提供其所有的独特服务。这种设计的优点是现在使 EC 自身与它可提供的服务的类型分离开。每个 SP 可藉此实

现其自身的服务能力。当另一 SP 替换卡上的 SP 时，不必对 EC 平台作任何改变。只需简单地把新的 SP 小应用程序载入卡中，新的 SP 小应用程序将执行所设计的功能。

在 SPDA 中，每个服务提供商都分配有存储公钥的空间。在许多交易中，只使用一对密钥，但是对于一些在线交易来说，需要两对或更多对的密钥。如果 SP 对于输入的消息和输出消息的签名都使用相同的公共密钥/专用密钥对，则一个公共密钥就足够了。如果 SP 对于签名使用不同的密钥，则在 SPDA 中需要两个 SP 公共密钥（一个用于输入消息，另一个用于输出消息的签名）。

在本发明的优选实施例中，使用两对公共密钥/专用密钥，而不是一对公共密钥/专用密钥，通过网络与其它应用程序通信，因为使用两对公共密钥/专用密钥比使用一对公共密钥/专用密钥的安全性更好。一对用于解密输入的消息，即，发送者利用接收者的公共密钥解密消息，接收者利用对应的专用密钥解密消息。另一对用于发送者对他发送的消息进行数字签名，接收者使用对应的发送者的公共密钥验证数字签名。

每个服务提供商分配有用于由服务提供商使用的许多公用密钥的空间。如果 SP 对于输入的消息和输出消息的签名都使用相同的公共密钥/专用密钥对，则一个公共密钥就足够了。如果对于接收消息和对消息签名，SP 使用不同的密钥对，则在 SPDA 中，两种 SP 的公共密钥都需要。

在本发明的一个备选实施例中，为了提供更高的交易安全性，服务提供商可能需要并使用两对以上的公共密钥/专用密钥。

当 EC 持卡人接受一个新的金融或非金融工具时，发行机构或信任的第三方将把包含记录的所需信息载入可用存储槽中。当服务提供商帐户被取消时，可消除该存储槽中的信息。在交易过程中，存储槽中的一些信息可被读取并被修改，例如帐户余额。诸如帐号之类的一些信息受到读保护，但是可被读取。诸如专用密钥之类的一些信息即不能读又不能写。存取条件 600 含有诸如 PIN，生物测量数据之类的

安全信息，为了打开卡，以便使用或者可以获得卡上存储的信息，EC用户必须提交这种安全信息。

传统的个人身份识别码（PIN）或者诸如生物测量数据之类的其它安全措施被用于保护 EC. 生物测定学涉及持卡人的生物特性，例如物体特征和行为特征的测量。生物测量系统可测量个人的指纹，手的几何形状，笔迹，面貌，语音，身体动作，击键节奏，眼睛特征，呼吸，体味，DNA 或者持卡人的任意其它身体属性。只有在所有存取条件已被满足之后，才可启动 EC 提供的功能。驻留在卡上的每个服务提供商可随意地实现其它存取条件。

图 4 表示了本发明的优选实施例的服务提供商数据区的格式。在表中，每个服务提供商的信息被分配一个表目，该表目可由附加的存取条件加以保护。PIN 712 和杂项数据字段 714 允许服务提供商要它所支持的工具提供额外的保护或数据字段。名称字段 702 含有服务提供商的名称，在开始在线交易时，持卡人可使用服务提供商的名称为交易选择适当的服务提供商。密钥类型字段 704 规定服务提供商选择使用的密钥的类型，保密密钥，公共密钥等等。密钥值 706 和帐户信息字段 708 含有每个服务提供商独有的信息。卡类型字段 710 规定服务提供商支持的工具的类型。

在本发明的优选实施例中，卡上操作系统（COS）为持卡人提供一些基本服务。下面是可由 COS 执行的大致功能的列表:

（1）诸如存储器管理，任务管理之类的传统 OS 功能。

（2）用户数据的外部通信-读/写和通信协议处理。

（3）卡上持卡人信息的装载和更新.

（4）用户 PIN 改变。

（5）诸如单个服务提供商信息的装载和更新之类的服务提供商数据区管理，SPDA 存取控制等等。

COS 还将在交易的各个阶段内提供支持。例如，COS 可在交易开始时处理 SP 选择，并当交易完成时，把交易记录到记录文件中。本发明的一个实施例可实现关于 COS 的下述两种设计途径之一，或者这两

种设计途径的混合。

（1）可把绝大多数情报放入 COS 中，COS 借此支持绝大多数的 EC 功能。从而，每个卡上服务提供商区域依赖于 COS 执行与商家和 SP 的交易。在这种途径中，COS 可为所有的卡上 SP 提供与外界的统一接口，并且一旦已选择 SP，能够有效地执行交易。

（2）或者，COS 可以是每个卡上 SP 可使用的一般性服务组合。每个 SP 数据区可含有小应用程序，这些小应用程序具有执行和商家及 SP 的交易所需的情报。在这种途径中，当执行交易时，SP 具有更多的机会实现其自己的独有特征。

图 5 表示了在本发明的优选实施例中，数据签名是如何被使用的。消息的发送者首先准备消息 M 的数据部分 900，并使其通过单向散列算法 H（*）902。散列算法的输出被称为消息 M 的消息摘要 MD 903。随后利用发送者的专用密钥（Pri）对 MD 加密，即数字签名，E（*）904。结果被称为消息 M 的数字签名 DS。随后结合该 DS 和初始消息 M 900，形成随时可通过网络 50 传输的完整消息 906。

公共密钥加密/解密函数可以是许多加密/解密函数中的任意加密/解密函数。其名字取自 RSA 开发者（Ronald Rivest，Adi Shamir 和 Len Adelman）姓的首个字母的 RSA 正是公共密钥加密/解密方法的一个例子，该加密/解密方法可被用在本发明的一个实施例中。

当预期的接收者从网络 50 收到消息时，他首先使消息 M 的数据部分 900 和与之相结合的数字签名 912 分开。随后，接收者使消息 M 的数据部分 900 通过相同的散列算法 910，散列算法 910 用于对消息 M 的数据部分 900 编码，从而得到消息 M 的消息摘要 MD^911。接收者随后利用发送者的公共密钥，对源始消息中所含的数字签名 912 解密，D（*）908，恢复初始的消息摘要，这里初始消息摘要被表示为 MD 909。把 MD 909 和新计算的 MD^911 进行比较。如果两者不相同，则初始消息已被破坏，并应被拒绝。

下面是图 5-11 中使用的符号和缩写的列表：

Acknowledgement $Data_{EC}$=由 EC 回送给 SP 的一部分消息。它通

知 SP 先前的消息已被成功地接收和处理。

Acknowledgement $Data_M$=由商家回送给 SP 的一部分消息，它通知 SP 先前的消息已被成功地接收和处理。

AI_{EC}=EC 持卡人的帐户信息。

AI_M=商家的帐户信息。

CRYPTO=密码。

D=解密功能。

$D_{SP\text{-}Private\text{-}key}$=利用 SP 的专用密钥进行解密。

DS=数字签名功能

$DS_{EC\text{-}Private\text{-}Key}$=由 EC 签在消息上的数字签名。

$DS_{M\text{-}Private\text{-}Key}$=由商家签在消息上的数字签名。

$DS_{SP\text{-}Private\text{-}Key}$=由 SP 签在消息上的数字签名。

E=加密功能。

E（Data）=使用数据加密密钥进行的数据加密。

$E_{SP\text{-}PK}$，$E_{SP\text{-}Public\text{-}Key}$=由 SP 公共密钥加密的数据。

$E_{Skey\text{-}EC}$，$D_{Skey\text{-}EC}$=利用 SP 为 EC 产生的对话密钥的加密/解密。

$E_{Skey\text{-}M}$，$D_{Skey\text{-}M}$=利用 SP 为商家产生的对话密钥的加密/解密。

EC=电子卡或电子卡等效软件

H（M）=对 M 应用单向散列算法。它产生 M 的消息摘要（MD）。

KE=密钥交换阶段。

M=商家

MD=消息摘要

MD^=由消息接受者利用刚接收的作为输入数据的消息，产生的消息摘要

MD_{EC}=从 EC 传至 SP 的消息的消息摘要

MD_M=从商家传至 SP 的消息的消息摘要。

$MD_{SP\text{-}M}$=从 SP 传至商家的消息的消息摘要。

$MD_{SP\text{-}EC}$=从 SP 传至 EC 的消息的消息摘要。该消息摘要由商家传递。

PLAIN TEXT: 明文，无需加密即可传送出的交易数据。明文可因不同的消息和交易方而有所不同。

PLAIN $TEXT_{EC}$: EC 在其输出消息中提供的部分交易数据。明文数据字段对安全性不敏感。于是，不需加密即可传送。注意当用在不同的消息中时，该符号的内容可不同。

PLAIN $TEXT_{M}$: 商家在其输出消息中提供的部分交易数据。明文数据字段对安全性不敏感。于是，不需加密即可传送。注意当用在不同的消息中时，该符号的内容可不同。

PLAIN $TEXT_{SP-EC}$: SP 在其输出消息中，仅仅提供给 EC 的交易数据的一部分。明文数据字段对安全性不敏感。于是，不需加密即可传送。注意当用在不同的消息中时，该符号的内容可不同。

PLAIN $TEXT_{SP-M}$: SP 在其输出消息中，仅仅提供给商家的交易数据的一部分。明文数据字段对安全性不敏感。于是，不需加密即可传送。注意当用在不同的消息中时，该符号的内容可不同。

STD=敏感的交易数据，在传送过程中需要加密。

STD_{EC}=由 EC 在其输出消息是提供的敏感交易数字数据。注意当用在不同的消息中时，该符号的内容可不同。

STD_{M}=由商家在其输出消息中提供的敏感交易数字数据。注意当用在不同的消息中时，该符号的内容可不同。

PK=公共密钥

EC-PK，PK_{EC}=电子卡的公共密钥

M-PK，PK_{M}=商家的公共密钥

SP-PK，PK_{SP}=选择的服务提供商的公共密钥

Response $Data_{SP-EC}$=SP-EC 交易响应数据: 在交易的交易阶段中，由 SP 回送给 EC 的一部分消息。它可包括批准/否决数据和/或任意其它相关数据。

Response $Data_{SP-M}$=SP-M 交易响应数据: 在交易的交易阶段中，由 SP 回送给商家的一部分消息。它可包括批准/否决数据和/或任意其它相关数据。

RN=随机数

RN_{EC}=由 EC 产生的，并被发送给 SP 的随机数。

RN_{SP-EC}=由 SP 产生的，并被发送给 EC 的随机数。

RN_M=由商家产生的随机数。

RN_{SP-M}=由 SP 产生的，并被发送给 M 的随机数。

SP=金融或非金融服务提供商。

TA=交易（货币）金额

交易识别号 $_{SP-EC}$，TID_{SP-EC}（交易 ID_{SP-EC}）=在交易的密钥交换阶段中，其值由 SP 分配的数据字段。在同一交易过程中，EC 将使用该值和 SP 通信。

交易识别号 $_{SP-M}$，TID_{SP-M}（交易 ID_{SP-M}）=在交易的密钥交换阶段中，其值由 SP 分配的数据字段。在同一交易过程中，商家将使用该值和 SP 通信。

* =在加密 E 或解密 D 中，数据的组合和级联。

图 6A-6Q 包括关于密码系统和方法的优选实施例的流程图。为了简化图 6A-6Q 中所含的说明和符号表示，流程图假定交易中所涉及的交易各方均使用一对密钥。在本发明的另一实施例中，可使用两对公共密钥，在这种情况下，这两对公共密钥均需要被交换。

本发明的优选实施例由不同的两个阶段组成：密钥交换阶段和交易阶段。

阶段 I：密钥交换阶段（握手协商阶段）

EC 持卡人把 EC 插入读/写卡器或者启动 EC 等效软件，并输入 PIN 码和/或满足存取条件 110，以便使用 EC 卡。把输入的安全信息条件与卡上信息 114 进行比较 112，以验证用户是否被授权使用该 EC 卡。如果安全信息和卡上的安全信息不匹配，则使用该 EC 卡的请求被拒绝 116。否则，该 EC 卡就会被开启 118，以供使用。一旦卡被开启，则用户可请求可供选择的卡上 SP 的列表，并通过向 EC 发出 SP 选择命令做出选择 120。一旦 SP 被选择，则 EC 进而开始与 SP 的密钥交换（KE）。从 EC 的 SPDA 得到由符号 SP-PK 和 PK_{SP} 代表的选择的

SP 的公共密钥，并用于对将发送给 SP 的消息加密。

KE 的主要目的是向 SP 安全地发送持卡人的公共密钥 PK_{EC}126 和 EC 随机数 RN_{EC}124. SP 对 EC 的响应将向 EC 赋予对话密钥和交易 ID，它们将由 EC 使用，以便在余下的交易过程中和 SP 通信。为了格式化 KE 消息，EC 产生随机数 RN_{EC}124，使之与 EC 的公共密钥 PK_{EC}126，以及与交易相关的和/或 SP 所要求的 EC 敏感交易数据 STD_{EC}128 级联。EC 利用从 SPDA 120 得到的 SP 的公共密钥 PK_{SP} 对它们加密 122。随后把得到的 EC 密码 $E_{ES\text{-}PK}$（RN_{EC}*PK_{EC}*STD_{EC}）和消息的明文部分 PLAIN $TEXT_{EC}$132（如果有的话）相结合 130，形成 EC 组合消息，PLAIN $TEXT_{EC}$*$E_{SP\text{-}PK}$（RN_{EC}*PK_{EC}*STD_{EC}）。当形成 EC 组合消息时，EC 的公共密钥 PK_{EC}126 可被放入明文 PLAIN $TEXT_{EC}$ 中，而不是被加密。

只有敏感数据才被加密。非敏感响应数据包括在明文中。只有 SP 才能够读取敏感数据。在多方交易中，SP 具有对所有交易者的敏感信息的完全存取权。

随后使得到的 EC 组合消息通过散列算法 134，形成散列消息，该散列消息是 EC 消息摘要 MD_{EC}。EC 136 利用 EC 专用密钥 138 对 EC 消息摘要 MD_{EC} 进行数字签名，形成数字签名消息 $DS_{EC\text{-}Private\text{-}Key}$。随后命名数字签名消息 $DS_{EC\text{-}Private\text{-}Key}$ 与 EC 组合消息结合 140。明文 PLAIN $TEXT_{EC}$，密码 $CRYPTO_{EC}$ 和数字签名 $DS_{EC\text{-}Private\text{-}Key}$ 是来自于 EC 的 KE 消息，并通过网络被发送给商家 158。明文包括所有各种非敏感的交易数据字段，于是可以清晰可辨的形式被传送；明文不需要加密。这些数据字段因各个消息而不同，并由交易各方确定。

为了和 SP 通信，商家格式化它自己与 SP 的 KE 消息所经历的步骤和 EC 格式化自己的与商家的 KE 消息所经历的步骤基本相同。持卡人和商家并不单独与 SP 通信，而是通过组合消息与 SP 通信。从而，在持卡人和商家之间，不必交换任何机密的金融信息。商家准备好他自己的用于交易的装置 142，并从驻留在商家的装置中的他自己的 SPDA 中，选择和 EC 持卡人已为该交易挑选的同一个 SP。从 SP 的

SPDA 中得到由符号 SP-PK 和 PK_{SP} 代表的 SP 的公共密钥，并用于对将发送给 SP 的消息加密。

为了格式化他自己的 KE 消息，商家产生随机数 RN148，使之与商家的公共密钥 PK_M150 和商家的敏感性交易数据 STD_M 级联，该敏感性交易数据是和交易相关的和/或 SP 152 所要求的数据。商家利用服务提供商 PK_{SP} 的公共密钥，对组合数据加密 146。随后使得到的密码与消息的明文部分 PLAIN $TEXT_M$156（如果有的话）组合 154，形成商家组合消息。当形成商家组合消息 PLAIN $TEXT_M$*E_{SP-PK}（RN_M*PK_M*STD_M）时，商家的公共密钥 PK_M150 可放入明文 PLAIN $TEXT_M$ 中，而不必被加密。

进一步使商家组合消息 [PLAIN $TEXT_M$*E_{SP-PK}（RN_M*PK_M*STD_M）]与 EC 的 KE 消息{[PLAIN $TEXT_{EC}$*E_{SP-PK}（RN_{EC}*PK_{EC}*STD_{EC}）]*$DS_{EC-Private-Key}$}组合 158，形成用于商家和 EC 的 KE 消息的数据部分，即，EC-商家组合消息{[PLAIN $TEXT_{EC}$*E_{SP-PK}（RN_{EC}*PK_{EC}*STD_{EC}）] * $DS_{EC-Private-Key}$} * [PLAIN $TEXT_M$ * E_{SP-PK}（RN_M*PK_M*STD_M）]。使 EC-商家组合消息通过散列算法 160，形成散列消息，该散列消息是商家消息摘要 MD_M。商家利用商家的专用密钥 164 对商家消息摘要 MD_M 进行数字签名 162，形成商家数字签名消息 $DS_{M-Private-Key}$。随后使商家数字签名消息 $DS_{M-Private-Key}$ 和消息的数据部分，即 EC-商家组合消息组合 166，形成商家和 EC 的密钥交换请求消息〈〈{[PLAIN $TEXT_{EC}$*E_{SP-PK}（RN_{EC}*PK_{EC}*STD_{EC}）] * $DS_{EC-Private-Key}$} * [PLAIN $TEXT_M$*E_{SP-PK}（RN_M*PK_M*STD_M）]〉〉 * $DS_{M-Private-Key}$。最后得到的消息通过网络被发送给 SP。图 7 表示了从商家到 SP 的密钥交换请求消息的最后格式和内容。

在本发明的优选实施例中，商家并不检查 EC 请求消息的 MD，即 MD_{EC}，因为 EC 已对其公共密钥进行了加密。但是，在备选实施例中，如果 EC 选择不对其公共密钥加密，则商家在把 EC 的 MD 传给 SP 之前，可随意地检查 EC 的 MD。在 EC 对其公共密钥加密或者 EC 不对其公共密钥加密的任一情况下，为了提高安全性，并防止商家可

能发生的处理错误，SP 仍然可以检查 EC 的 MD。当商家从 SP 收到发给他自己和 EC 的组合响应时，商家不必为 EC 检查 MD，因为该 MD 是由单个发起者-SP 形成的整个消息的一部分。商家只需检查他从 SP 收到的整个消息的 MD。

当 SP 收到 KE 请求消息时，SP 首先使 KE 请求消息的数据部分和 DS 分开 168，并把 KE 请求消息的数据部分送入单向散列算法，以便重新计算消息摘要，该消息摘要变成 MD_M。随后 SP 分离商家的明文 PLAIN $TEXT_M$，密码 $CRYPTO_M$，数字签名 $DS_{M\text{-}Private\text{-}Key}$ 和 EC 的 KE 请求消息 PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$*$DS_{EC\text{-}Private\text{-}Key}$。通过利用其自己的专用密钥，SP 对商家的密码 170 解密，并且除了其它信息之外还恢复商家的随机数 RN_M148 和商家的公共密钥 PK_M150。随后 SP 使用恢复的 PK_M 对商家签名的数字签名 $DS_{M\text{-}Private\text{-}Key}$ 解密，并恢复商家的 KE 消息的 MD_M。SP 把散列得到的新 $MD^{\wedge}_M$168 和通过对 DS 解密，从原始的 KE 消息恢复的 MD_M170 进行比较 172。如果 $MD^{\wedge}_M$ 和 MD_M 之间存在差异，则 KE 消息已被破坏，于是该 KE 消息被拒绝 174。如果 $MD^{\wedge}_M$ 和 MD_M 匹配，则 SP 使 EC 的 KE 请求消息的数据部分与 DS 分开，并把 EC 的 KE 请求消息的数据部分送入单向散列算法，以便重新计算消息摘要（$MD^{\wedge}_{EC}$）。随后在步骤 176，SP 分离 EC 的 KE 请求消息的数据部分中的 EC 的明文 PLAIN $TEXT_{EC}$（如果有的话），密码 $CRYPTO_{EC}$，和数字签名 $DS_{EC\text{-}Private\text{-}Key}$。通过利用其自己的专用密钥，SP 对 EC 的密码解密，并且除了其它消息之外还恢复 EC 的随机数 RN_{EC} 和 EC 的公共密钥 PK_{EC}。随后 SP 利用恢复的 PK_{EC} 对 EC 签名的数字签名解密，并恢复 EC 的 KE 消息的 MD_{EC}。在步骤 718 中，SP 把散列得到的新 $MD^{\wedge}_{EC}$176 和通过对 DS 解密，从原始的 KE 消息中恢复的 MD_{EC} 进行比较。如果 $MD^{\wedge}_{EC}$ 和 MD_{EC} 之间存在差异，则 KE 消息已被破坏，于是 KE 消息被拒绝 180。否则，SP 准备向商家和 EC 回送 KE 响应消息。

为了格式化给 EC 的 KE 响应消息，SP 产生一个随机数 $RN_{SP\text{-}EC}$184，和给 EC 的对话密钥 $Skey_{EC}$186，并使它们与 EC 产生的随机

数 RN_{EC}188，服务提供商敏感交易数据 STD_{SP-EC}190 结合，并利用 EC 的公共密钥 PK_{EC} 对它们加密 192。所得到的密码 E_{EC-PK}（RN_{EC}*RN_{SP-EC}*$Skey_{EC}$*STD_{SP-EC}）与 SP 分配给 EC 的交易识别号 TID_{SP-EC}194，和明文 PLAIN $TEXT_{SP-EC}$195（如果有的话）组合 196，形成发给 EC 的响应消息的数据部分。SP 使该数据通过散列算法，以便计算消息摘要 MD_{SP-EC}198。通过利用其自己的专用密钥 202，SP 通过对消息摘要 MD_{SP-EC} 进行数字签名，为响应消息产生数字签名 $DS_{SP-Private-Key}$200。在使该消息的数据部分与计算得到的新的 $DS_{SP-Private-Key}$ 组合 204 之后，完成 SP 发给 EC 的 KE 响应消息[TID_{SP-EC}* PLAIN $TEXT_{SP-EC}$* E_{EC-PK}（RN_{EC}*RN_{SP-EC}*$Skey_{EC}$*STD_{SP-EC}）]* $DS_{SP-Private-Key}$。

为了格式化给商家的 KE 响应消息，SP 产生随机数 RN_{SP-M}208，和给商家的对话密钥 $Skey_M$210，并使它们与商家产生的随机数 RN_M212，敏感交易数据 STD_{SP-EC}214 结合，并利用在步骤 170 接收的商家的公共密钥 PK_M 对它们加密 206。使所得到的密码由与 SP 分配给商家的交易识别号 TID_{SP-M}218，和明文 PLAIN $TEXT_{SP-M}$220（如果有的话）组合 216，形成发给商家的响应消息的数据部分。所得到的组合消息 TID_{SP-M}*PLAIN $TEXT_{SP-M}$*E_{M-PK}（RN_{SP-M}*RN_M*$Skey_M$*STD_{SP-M}）进一步与发给 EC 的 KE 响应消息[TID_{SP-EC}* PLAIN $TEXT_{SP-EC}$* E_{EC-PK}（RN_{EC}*RN_{SP-EC}*$Skey_{EC}$*STD_{SP-EC}）]* $DS_{SP-Private-Key}$。组合 222，形成 SP 的最终 KE 响应消息的数据部分，[TID_{SP-EC}* PLAIN $TEXT_{SP-EC}$* E_{EC-PK}（RN_{EC}*RN_{SP-EC}*$Skey_{EC}$*STD_{SP-EC}）]* $DS_{SP-Private-Key}$*[TID_{SP-M}*PLAIN $TEXT_{SP-M}$*E_{M-PK}（RN_{SP-M}*RN_M*$Skey_M$*STD_{SP-M}）]。SP 使该数据部分通过散列算法，以便计算消息摘要 224。通过利用其自己的专用密钥 228，SP 通过对该消息摘要进行数字签名，为响应消息产生数字签名 $DS_{SP-Private-Key}$226。在使该消息的数据部分与计算得到的新的 DS 226 组合 230 之后，完成发给 EC 和商家的 KE 响应消息。该响应消息〈〈{[TID_{SP-EC}* PLAIN $TEXT_{SP-EC}$*（E_{EC-PK}*RN_{EC}*RN_{SP-EC}*$Skey_{EC}$*STD_{SP-EC}）]* $DS_{SP-Private-Key}$}*[TID_{SP-M}*PLAIN $TEXT_{SP-M}$* E_{M-PK}（RN_{SP-M}*RN_M*$Skey_M$*STD_{SP-}

$_M$）]〉〉 $DS_{SP\text{-}Private\text{-}Key}$ 通过网络被回送给商家。图 8 表示了从 SP 到商家的组合 KE 响应消息的最终格式和内容。

当商家收到 KE 响应消息 232 时，商家首先分离由 SP 签名的 $DS_{SP\text{-}Private\text{-}Key}$，随后把组合 KE 响应消息的数据部分送入单向散列算法，以便重新计算消息摘要 $MD^{\wedge}_{SP\text{-}M}$。随后商家分离 SP 的 KE 响应消息的数据部分，即，$TID_{SP\text{-}M}$，$PLAIN\ TEXT_{SP\text{-}M}$，$CRYPTO_{SP\text{-}M}$，[（$TID_{SP\text{-}EC}$* $PLAIN\ TEXT_{SP\text{-}EC}$* $CRYPTO_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$。商家使用 SP 的公共密钥（选自 144）对数字签名 $DS_{SP\text{-}Private\text{-}Key}$ 解密，恢复消息摘要 $MD_{SP\text{-}M}$。商家把散列得到的新的 $MD^{\wedge}_{SP\text{-}M}$ 与 MD_{EC} 进行比较 234。如果在 $MD^{\wedge}_{SP\text{-}M}$ 和 $MD_{SP\text{-}M}$ 之间存在任何差异，则 KE 响应消息已被破坏，于是被拒绝 236。如果 $MD^{\wedge}_{SP\text{-}M}$ 和 $MD_{SP\text{-}M}$ 匹配，则商家识别意欲发送给他的响应消息部分，并利用他自己的专用密钥对密码 $CRYPTO_{SP\text{-}M}$ 解密 238。商家应能够恢复他在 KE 请求消息中发送给 SP 的原始随机数 RN_M（见步骤 148）。在步骤 240 中，商家把恢复的随机数 RN_M（步骤 238）与原始的随机数 RN_M 进行比较。如果两值不相等，则消息已被破坏，在步骤 242 拒绝该消息。由于随机数 RN_M 只有 SP 利用正确的 SP 专用密钥才能恢复，因此确定消息的发送者真正地是所选的 SP。随后商家把 EC 的 KE 响应消息[（$TID_{SP\text{-}EC}$* $PLAIN\ TEXT_{SP\text{-}EC}$* $CRYPTO_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$ 转发给 EC，并为交易的交易阶段做准备。

当 EC 收到 KE 响应消息 260 时，EC 首先分离由 SP 签名的 $DS_{SP\text{-}Private\text{-}Key}$，随后把给 EC 的 KE 响应消息的数据部分送入单向散列算法，产生 $MD^{\wedge}_{SP\text{-}EC}$。随后 EC 分离该消息的数据部分，即，$TID_{SP\text{-}EC}$，$PLAIN\ TEXT_{SP\text{-}EC}$，$CRYPTO_{SP\text{-}EC}$，$DS_{SP\text{-}Private\text{-}Key}$。EC 使用 SP 的公共密钥（在步骤 120 中选择）对数字签名 $DS_{SP\text{-}Private\text{-}Key}$ 消息解密，恢复消息摘要 MD_{SP}。EC 把散列得到的新的 $MD^{\wedge}_{SP\text{-}EC}$（在步骤 260 中得到）与通过对 $DS_{SP\text{-}Private\text{-}Key}$ 解密，从给 EC 的 KE 响应消息中恢复的 $MD_{SP\text{-}EC}$ 进行比较 262。如果在 $MD^{\wedge}_{SP\text{-}EC}$ 和 $MD_{SP\text{-}EC}$ 之间存在任何差异，则发给 EC 的 KE 响应消息已被破坏，于是在步骤 264 被拒绝。如果 $MD^{\wedge}_{SP\text{-}M}$

和 MD_{SP-M} 匹配，则 EC 识别意欲发送给他的响应消息部分，并利用他自己的专用密钥对包含在该消息中的密码 $CRYPTO_{SP-EC}$ 解密 266。EC 应能够恢复在 EC 的 KE 请求消息中发送的原始随机数 RN_{EC}（见步骤 124）。在步骤 268 中，EC 把恢复的随机数 RN_{EC}（步骤 266）与原始的随机数 RN_{EC}（步骤 124）进行比较。如果这两个随机数不相等，则消息已被破坏，在步骤 270 拒绝该消息。由于只有 SP 利用正确的 SP 专用密钥才能够恢复随机数 RN_{EC}，因此这可确保消息的发送者真正地是所选的 SP。EC 为交易的交易阶段做准备。

在 EC 和商家中将有一个预选确定的超时期。在交易中，如果在超时期内没有收到响应消息，则 EC 和商家将认为该交易被放弃，并将进行重试或者启动恢复进程。

在成功地完成 KE 消息交换之后，SP 具有 EC 的公共密钥和商家的公共密钥。这时，EC 和商家都具有来自于 SP 的随机数，交易 ID 和对话密钥。为了完成交易的密钥交换阶段，EC 和商家必须把从 KE 响应消息恢复的这两个随机数回送给 SP。这可以两个方式实现。可借助来自于 EC 和商家的确认消息回送随机数。或者随机数可作为从 EC 和商家输出的，传到 SP 的下一消息，例如交易消息一部分被回送。第二种方法较简单，并在下面的阶段 II 中进行说明。为了确保 SP 和商家之间，以及 SP 和 EC 之间密钥交换的正确性，随机数只被使用一次。一旦已建立对话密钥和交易识别号，就不再使用随机数。

阶段 II: 交易阶段

在交易阶段中，商家和 EC 均向 SP 发送他们自己的诸如帐号之类的帐户信息，以及其它和交易相关的数据，例如交易金额，请求批准交易或者其它处理数据。同样，EC 和商家单独地与 SP 商谈，不过是通过组合消息与 SP 商谈，商家负责组合消息，并把组合后的消息作为一个消息发送给 SP。

EC 首先通过使来自于 SP 的随机数 RN_{SP-EC}274 和与选择的 SP 有关的 EC 帐户信息，AI_{EC}276，交易金额 TA 280，以及与交易相关的和/或 SP 要求的任意其它敏感数据 278 级联，形成交易消息。EC 利用

SP 分配的对话密钥 $Skey_{EC}$ 对它们加密。$Skey_{EC}$ 是保密密钥，并使用和用于公共密钥加密的加密算法不同的加密算法。随后在步骤 282，使所得到的密码 $CRYPTO_{EC}$，即 $Skey_{EC}$（RN_{SP-EC}*STD_{EC}*AI_{EC}*TA）与交易 ID TID_{SP-EC}284 和明文 PLAIN $TEXT_{EC}$286（如果有的话）组合，形成 EC 的交易消息的数据部分，TID_{SP-EC}*PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$。数据部分 282 被输入单向散列算法 288，以便计算消息摘要 MD_{EC}，随后利用 EC 的专用密钥 292 对该消息摘要 MD_{EC} 进行数字签名 290。在步骤 294，使得到的数字签名 290 与消息的数据部分（来自于步骤 282）组合，形成 EC 的交易请求消息[TID_{SP-EC}* PLAIN $TEXT_{EC}$*$Skey_{EC}$（RN_{SP-EC}*STD_{EC}*AI_{EC}*TA）]*$DS_{EC-Private-Key}$，随后将其发送给商家。

商家经历基本相同的步骤，形成他的交易消息。商家通过使来自于 SP 的随机数 RN_{SP-M}246 和与选择的 SP 有关的商家帐户信息，AI_M248，交易金额 TA 252，以及与交易相关的和/或 SP 要求的任意其它敏感数据 STD_M250 级联，形成他的交易消息。商家利用 SP 分配的对话密钥 $Skey_M$ 对它们加密 244。对话密钥 $Skey_{EC}$ 是保密密钥，并通过利用和用于公共密钥加密的加密算法不同的加密算法，例如 DES 产生。对话密钥 $Skey_M$ 用于在此时执行加密，以产生密码 $CRYPTO_M$。随后在步骤 254，使所得到的密码 $CRYPTO_M$，即 $Skey_M$（RN_{SP-M}*STD_M*AI_M*TA）与交易 ID TID_{SP-M}256 和明文 PLAIN $TEXT_M$258（如果有的话）组合，形成商家的交易消息的数据部分，TID_{SP-M}*PLAIN $TEXT_M$*$CRYPTO_M$。在步骤 296，使该数据与 EC 的交易请求组合，形成给 SP 的最终交易请求消息的数据部分，[TID_{SP-EC}* PLAIN $TEXT_{EC}$*$Skey_{EC}$（RN_{SP-EC}*STD_{EC}*AI_{EC}*TA）]*$DS_{EC-Private-Key}$*[TID_{SP-M}*PLAIN $TEXT_M$* $Skey_M$（RN_{SP-M}*STD_M*AI_M*TA）]。和前面一样，商家把他的组合数据输入单向散列算法 298，以计算消息摘要 MD_M，随后利用商家的专用密钥 302 对该消息摘要 MD_M 进行数字签名 300。在步骤 304，使得到的数字签名 $DS_{M-Private-Key}$300 与消息的数据部分（来自于步骤 296）组合，形成最终的交易请求消息{[TID_{SP-EC}* PLAIN

$TEXT_{EC}$* $Skey_{EC}$（RN_{SP-EC}*STD_{EC}*AI_{EC}*TA）]*$DS_{EC-Private-Key}$*[TID_{SP-M}*PLAIN $TEXT_M$* $Skey_M$（RN_{SP-M}*STD_M*AI_M*TA）]}* $DS_{M-Private-Key}$，随后将其发送给 SP。图 9 表示了交易请求消息的最终格式。

当 SP 收到交易请求消息时，SP 首先检查 EC 和商家发送的这两个交易识别号，即，TID_{SP-EC} 和 TID_{SP-M}，确保它们是有效的。当在步骤 306 发现或者 TID_{SP-M}（步骤 210）或者 TID_{SP-EC}（步骤 186）无效时，则在步骤 308 拒绝该消息。如果交易识别号都有效，则 SP 着手使 $DS_{M-Private-Key}$ 和消息的数据部分分开，并把消息的数据部分，{[TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$（RN_{SP-EC}*STD_{EC}*AI_{EC}*TA）]*$DS_{EC-Private-Key}$ *[TID_{SP-M}*PLAIN $TEXT_M$* $Skey_M$（RN_{SP-M}*STD_M*AI_M*TA）]}输入单向散列算法，以计算该消息的消息摘要 MD ^$_M$。SP 分离消息的数据部分，即 TID_{SP-M}，PLAIN $TEXT_M$，$CRYPTO_M$，$DS_{M-Private-Key}$，（TID_{SP-EC}*PLAIN $TEXT_{EC}$*$CRYPTO_{EC}$）*$DS_{EC-Private-Key}$。SP 利用商家的公共密钥对 $DS_{M-Private-Key}$ 加密 310，并把新恢复的消息摘要 MD_M 和刚计算的消息摘要 MD ^$_M$（步骤 306）进行比较。如果 MD ^$_M$ 和 MD_M 不等，则消息已被破坏，于是在步骤 314 被拒绝。如果 MD ^$_M$ 和 MD_M 匹配，则 SP 利用它在 KE 阶段中分配给商家的对话密钥 $Skey_M$（步骤 210）对消息的加密部分解密 316，并恢复加密部分中所含的数据字段。在步骤 318，SP 把商家在消息中回送的随机数 RN_{SP-M} 和 SP 最初发送给商家的消息中的随机数 RN_{SP-M}（见步骤 208）进行比较。如果两个随机数不相等，则商家没有通过相互的验证测试，于是在步骤 320，拒绝该消息。

另外，SP 将验证 EC 的帐户信息 AI_{EC} 和诸如交易金额 TA 之类的交易数据。如果 AI 不再有效，则在步骤 320 拒绝该消息。当来自 EC 的 TA 和来自商家的 TA 不相符时，该消息也将被拒绝。可具有使消息无效的其它条件。如果帐户信息 AI_{EC} 和交易数据是有效的，则 SP 继续验证消息的 EC 部分。

正如商家的消息的情况一样，SP 首先使 $DS_{EC-Private-Key}$ 和 EC 的消息分开 322，并把 EC 的消息的数据部分（TID_{SP-EC}*PLAIN

$TEXT_{EC}$*$CRYPTO_{EC}$）输入单向散列算法，以计算 EC 消息的消息摘要 $MD^{\wedge}_{EC}$。SP 分离 EC 的交易请求的数据部分，$TID_{SP\text{-}EC}$，PLAIN $TEXT_{EC}$，$CRYPTO_{EC}$，$DS_{EC\text{-}Private\text{-}Key}$。SP 利用 EC 的公共密钥 PK_{EC} 对 $DS_{EC\text{-}Private\text{-}Key}$ 解密 324，并恢复 MD_{EC}。在步骤 326，SP 把恢复的 MD_{EC} 和 $MD^{\wedge}_{EC}$ 进行比较。如果 $MD^{\wedge}_{EC}$ 和 MD_{EC} 不等，则消息已被破坏，于是在步骤 328 拒绝该消息。如果 $MD^{\wedge}_{EC}$ 和 MD_{EC} 相符，则 SP 利用它在 KE 阶段中分配给 EC 的对话密钥 $Skey_{EC}$（步骤 186），对 EC 消息的加密部分解密 330，并恢复该加密部分中所含的数据字段。在步骤 332，SP 把 EC 在消息中回送的随机数 $RN_{SP\text{-}EC}$ 和 SP 最初发送给 EC 的随机数 $RN_{SP\text{-}EC}$（步骤 184）进行比较。如果随机数不等，则 EC 未能通过相互的验证测试，于是在步骤 334 拒绝该消息。SP 将验证商家的帐户信息 AI_M 和诸如交易金额 TA 之类的交易数据，当帐户信息无效，或者当交易数据不满足 SP 的标准时，在步骤 334 将拒绝该消息。一旦已确立整个消息的完整性和真实性，则 SP 可处理消息中所含的数据，并回送响应消息。在该消息中回送的随机数终结 SP 和商家之间的相互验证，以及 SP 和 EC 之间的相互验证。在该消息之后，不再需要执行任何随机数的交换。SP 可选择把随机数用作交易识别号，在商家和 EC 发送给 SP 的所有后续消息中，商家和 EC 将使用该交易识别号。

和前面一样，响应消息含有回复给 EC 和商家的信息。为了格式化回复给EC的交易响应消息，SP产生回复给EC的响应数据，Response $Data_{SP\text{-}EC}$338，并利用分配给 EC 的对话密钥 $Skey_{EC}$ 对其加密 336。只有敏感性数据才被加密。非敏感性响应数据包含在明文中。在步骤 340，使密码 $CRYPTO_{SP\text{-}EC}$，即 $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）和 SP 分配给 EC 的交易识别号 $TID_{SP\text{-}EC}$342（步骤 194），以及 SP 要回复给 EC 的明文 PLAIN $TEXT_{SP\text{-}EC}$344（如果有的话）结合，形成要回复给 EC 的响应消息的数据部分，即，$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）。把该消息的数据部分输入散列算法 346，产生 SP 利用 SP 的专用密钥 350 对其进行数字签名 348 的 $MD_{SP\text{-}EC}$。在步

骤 352，使 $DS_{SP\text{-}Private\text{-}Key}$和响应消息的数据部分（步骤 340）结合，形成要回复给 EC 的完整响应消息，[$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$。

为了格式化要回复给商家的交易响应消息，SP 产生要回复给商家的响应数据，Response $Data_{SP\text{-}M}$356，并利用分配给商家的对话密钥 $Skey_M$（步骤 210）对其加密 354。在步骤 358，使密码 $CRYPTO_{SP\text{-}M}$与在步骤 360 分配给商家的交易识别号 $TID_{SP\text{-}M}$（步骤 218），以及 SP 要回复给商家的明文 PLAIN $TEXT_{SP\text{-}M}$（如果有的话）362 结合，形成要回复给商家的响应消息的数据部分，$TID_{SP\text{-}M}$* PLAIN $TEXT_{SP\text{-}M}$* $CRYPTO_{SP\text{-}M}$。随后在步骤 364 使该数据与要回复给 EC 的完整的响应消息结合，形成要回复给 EC 和商家的响应消息的数据部分，[$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$*[$TID_{SP\text{-}M}$* PLAIN $TEXT_{SP\text{-}M}$* $E_{Skey\text{-}M}$（Response $Data_{SP\text{-}M}$）]。

随后把该数据输入散列算法 366，产生 SP 利用 SP 的专用密钥 370 对其数字签名 368 的 $MD_{SP\text{-}M}$。在步骤 372，使 $DS_{SP\text{-}Private\text{-}Key}$和要回复给 EC 和商家的响应消息的数据部分结合，形成要回复给 EC 和商家的完整的响应消息，〈〈{[$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$}*[$TID_{SP\text{-}M}$* PLAIN $TEXT_{SP\text{-}M}$* $E_{Skey\text{-}M}$（Response $Data_{SP\text{-}M}$）]〉〉 $DS_{SP\text{-}Private\text{-}Key}$。随后 SP 把其响应消息回送给商家。图 10 表示了交易响应消息的最终格式。

当商家收到该消息时，商家首先在步骤 374 检查消息中的交易识别号 $TID_{SP\text{-}M}$，并确保该交易识别号有效。如果交易识别号无效，则在步骤 376 拒绝该消息。如果 $TID_{SP\text{-}M}$有效，则商家使被 SP 签名的 $DS_{SP\text{-}Private\text{-}Key}$和该消息的数据部分分开，随后把交易响应消息的数据部分〈〈{[$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）]* $DS_{SP\text{-}Private\text{-}Key}$}*[$TID_{SP\text{-}M}$* PLAIN $TEXT_{SP\text{-}M}$* $E_{Skey\text{-}M}$（Response $Data_{SP\text{-}M}$）]〉〉输入单向散列算法，产生 $MD_{SP\text{-}M}$。商家把消息的数据部分分离成不同的部分，$TID_{SP\text{-}M}$，PLAIN $TEXT_{SP\text{-}M}$，$CRYPTO_{SP\text{-}M}$，$DS_{SP\text{-}Private\text{-}Key}$（$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $CRYPTO_{SP\text{-}EC}$* $DS_{SP\text{-}Private\text{-}Key}$），

并准备把 SP 的交易响应消息传发给 EC。在步骤 378，商家利用在 KE 阶段中，由 SP 分配的对话密钥 $Skey_M$，对 SP 的消息的加密部分解密，并恢复其中所含的数据字段。随后商家使用 SP 的公共密钥，PK_{SP}（步骤 144），对数字签名 $DS_{SP\text{-}Private\text{-}Key}$ 解密，以便恢复 $MD_{SP\text{-}M}$。在步骤 380，商家把散列得到的新的 $MD^{\wedge}_{SP\text{-}M}$（步骤 374）和恢复的 $MD_{SP\text{-}M}$ 进行比较。如果 $MD^{\wedge}_{SP\text{-}M}$ 和 $MD_{SP\text{-}M}$ 不符，则交易响应消息已被破坏，于是在步骤 382 拒绝该消息。如果这两个消息摘要相符，则商家开始处理该消息。照常，把交易响应消息的 EC 部分（$TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $CRYPTO_{SP\text{-}EC}$* $DS_{SP\text{-}Private\text{-}Key}$）传给 EC。

当 EC 收到交易响应消息时，EC 首先在步骤 394 检查消息中的交易识别号 $TID_{SP\text{-}EC}$，并确保该交易识别号有效。如果交易识别号无效，则在步骤 396 拒绝该消息。如果交易识别号有效，则商家使被 SP 签名的 $DS_{SP\text{-}Private\text{-}Key}$ 和交易响应消息的数据部分分开，随后把 EC 交易响应消息的数据部分 $TID_{SP\text{-}EC}$* PLAIN $TEXT_{SP\text{-}EC}$* $E_{Skey\text{-}EC}$（Response $Data_{SP\text{-}EC}$）输入单向散列算法，产生 $MD^{\wedge}_{SP\text{-}EC}$。EC 把消息分离成不同的部分，$TID_{SP\text{-}EC}$，PLAIN $TEXT_{SP\text{-}EC}$，$CRYPTO_{SP\text{-}EC}$，$DS_{SP\text{-}Private\text{-}Key}$。在步骤 398，EC 利用在 KE 阶段中，由 SP 分配的对话密钥 Skey，对 SP 的消息的加密部分解密，并恢复其中所含的数据字段。EC 使用 SP 的公共密钥（步骤 120）对数字签名 $DS_{SP\text{-}Private\text{-}Key}$ 解密，以便恢复消息摘要 $MD_{SP\text{-}EC}$。在步骤 400，商家把散列得到的新的 $MD^{\wedge}_{SP\text{-}EC}$394 和恢复的 $MD_{SP\text{-}EC}$ 进行比较。如果 $MD^{\wedge}_{SP\text{-}EC}$ 和 $MD_{SP\text{-}EC}$ 不符，则交易响应消息已被破坏，于是在步骤 402 拒绝该消息。如果这两个消息摘要相符，则 EC 开始处理该消息。

在交易的最后，如果 SP 要求的话，EC 和商家可向 SP 发送确认消息，通知响应消息已被正确地接收和处理。如果在交易结束之前，在 SP 和商家及 EC 之间，将交换多个消息，则该确认数据可作为要发送给 SP 的下一消息的一部分。或者确认数据单独成为一个消息。

为了格式化确认消息，EC 首先在步骤 404，利用对话密钥 $Skey_{EC}$ 对确认数据 Acknowledgement $Data_{EC}$406（如果有的话）的敏感部分

加密，从而产生 $Skey_{EC}$（Acknowledgement $Data_{EC}$）。在步骤 408，EC 把得到的密码和由 SP 分配的交易识别号 TID_{SP-EC}410，以及明文 PLAIN $TEXT_{EC}$412（如果有的话）结合。形成 EC 的确认消息的数据部分，TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$（Acknowledgement $Data_{EC}$）。随后把该组合数据输入单向散列算法 414，产生 MD_{EC}。随后 EC 利用 EC 的专用密钥 418 对得到的 MD_{EC} 进行数字签名 416，产生 $DS_{EC-Private-Key}$。在步骤 420，使 $DS_{EC-Private-Key}$ 和消息的数据部分（来自于步骤 408）结合，形成 EC 的完整的确认消息，[TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$（Acknowledgement $Data_{EC}$）]* $DS_{EC-Private-Key}$。随后把该确认消息发送给商家。

商家经历相同的步骤，形成他自己的确认消息。为了格式化确认消息，商家首先利用 SP 分配给商家的对话密钥 $Skey_M$ 对确认数据 Acknowledgement $Data_M$386（如果有的话）的敏感部分加密，从而产生 $Skey_M$（RN_{SP-M}*Acknowledgement $Data_M$）。在步骤 388，商家把得到的密码和 SP 分配的交易识别号 TID_{SP-M}390，以及明文 PLAIN $TEXT_M$（来自于步骤 392）（如果有的话）结合。形成商家的确认消息的数据部分，TID_{SP-M}* PLAIN $TEXT_M$* $Skey_M$（RN_{SP-M}*Acknowledgement $Data_M$）。在步骤 422，使该数据部分进一步和从 EC 接收的确认消息结合，形成要发送给 SP 的组合确认消息的数据部分，{[TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$(Acknowledgement $Data_{EC}$)]* $DS_{EC-Private-Key}$}*[TID_{SP-M}* PLAIN $TEXT_M$* $Skey_M$（Acknowledgement $Data_M$）]。商家把要发送给 SP 的组合确认消息的数据部分输入单向散列算法，产生消息摘要 MD_M。随后商家利用商家的专用密钥 428 对得到的 MD_M 进行数字签名，产生 $DS_{M-Private-Key}$ 426。在步骤 430，使 $DS_{M-Private-Key}$ 和消息的数据部分（来自于步骤 422）结合，形成要发送给 SP 的 EC 和商家的最终的组合确认消息，〈〈{[TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$（Acknowledgement $Data_{EC}$）]* $DS_{EC-Private-Key}$}*[TID_{SP-M}* PLAIN $TEXT_M$* $Skey_M$(Acknowledgement $Data_M$)]〉〉*$DS_{M-Private-Key}$。随后把该消息发送给 SP。图 11 表示了交易确认消息

的最终格式。

TID_{SP-M}是SP分配给商家的交易识别号(来自于步骤218), TID_{SP-EC}是SP分配给EC的交易识别号(来自于步骤194)。当收到交易确认消息时，SP在步骤432检查由EC和商家发送的这两个交易识别号TID_{SP-M}和TID_{SP-EC}，并确保它们有效。当发现TID_{SP-M}或TID_{SP-EC}无效时，则在步骤434拒绝该消息。如果交易识别号都有效，则SP着手使$DS_{M-Private-Key}$和组合的确认消息分开，并把组合的确认消息的数据部分〈〈{[TID_{SP-EC}* PLAIN $TEXT_{EC}$* $Skey_{EC}$(Acknowledgement $Data_{EC}$)]* $DS_{EC-Private-Key}$}*[TID_{SP-M}* PLAIN $TEXT_M$* $Skey_M$(Acknowledgement $Data_M$)]〉〉输入单向散列算法，以便计算该消息的消息摘要$MD^{\wedge}_M$。SP把消息的数据部分分离成TID_{SP-M}，PLAIN $TEXT_M$，$CRYPTO_M$，$DS_{M-Private-Key}$，(TID_{SP-EC}* PLAIN $TEXT_{EC}$* $CRYPTO_{EC}$)*$DS_{EC-Private-Key}$。在步骤436，SP利用商家的公共密钥PK_M对$DS_{M-Private-Key}$解密，并把恢复的消息摘要MD_M432和刚计算的消息摘要$MD^{\wedge}_M$436进行比较。如果$MD^{\wedge}_M$和MD_M相符，则SP在步骤442，利用它在KE阶段中，分配给商家的对话密钥$Skey_M$(来自于步骤210)，对商家的确认消息的加密部分解密，并恢复其中所含的确认数据。

在步骤444，SP使$DS_{EC-Private-Key}$和EC的确认消息分开，并把EC的确认消息的数据部分TID_{SP-EC}* PLAIN $TEXT_{EC}$* $CRYPTO_{EC}$输入单向散列算法，以计算该消息的消息摘要$MD^{\wedge}_{EC}$。SP把EC的确认消息的数据部分分离成TID_{SP-EC}，PLAIN $TEXT_{EC}$，$CRYPTO_{EC}$，$DS_{EC-Private-Key}$。在步骤446，SP利用EC的公共密钥PK_{EC}对$DS_{EC-Private-Key}$解密，并在步骤448，把恢复的MD_{EC}和刚计算的消息摘要$MD^{\wedge}_{EC}$444进行比较。如果这两个消息摘要相符，则SP在步骤452，利用它在KE阶段中，分配给EC的对话密钥$Skey_{EC}$(来自于步骤186)，对该消息的加密部分解密，并恢复其中所含的确认数据。随后在步骤454，结束交易的交易阶段的处理。

在整个交易过程中，在优选实施例中，EC使用由诸如Microsoft Explorer或Netscape Navigator之类的因特网浏览器软件提供的软

件。在一个典型的对话期中，持卡人使其浏览器指向商家的 URL，并从商家定购货物或服务。在支付费用时，浏览器将调用 EC 接口软件，EC 接口软件可嵌入浏览器中，或者作为插入式可附加软件成分包括于其中，并允许交易继续进行。持卡人可把他的浏览器指向任意 SP 会员的 URL。

上面在图 6A-6Q 中描述的两阶段交易只是应用本发明的两阶段密钥交换-交易模式的一个特例。在图 6A-6Q 中描述的两阶段交易中，参加交易的交易者一共有三位：EC，商家和 SP。两阶段密钥交换-交易模式类似地可适用于涉及的交易方的数目为二位到多位不等。在涉及的交易者多于三位的交易中，只有一方担任 SP 的角色。所有其它各方使用选定的 SP 的公共密钥执行初始的密钥交换，并使用 SP 分配的对话密钥和交易 ID 进行交易。

两阶段密钥交换-交易模式适用于组织方案，其中（1）交易参加者可被安排成和可能的多个路由器与服务提供商串联排列；或者（2）交易参加者可和可能的路由器被安排在分层组织中。这些额外的组织方案可涉及把消息送到下一层次的路由器。分层结构中的一个层次可由任意数目的交易参加者和/或路由器组成。下一层次是在顺序上或者层次上邻接的下一交易参加者或路由器。在分层组织方案中，下一层次包括所有可能的下一交易参加者和路由器。对于分层组织方案来说，SP 建立用于确定消息将被发送给它的下一交易参加者或路由器的准则。

路由器是网关/管道，它收集来自前一层次的消息，并按照诸如组合消息之类的 SP 要求，对消息进行某些处理，随后把消息转给 SP。每个交易参加者只需形成他自己的消息（数据和数字签名），并将其发送给下一层次。交易参加者把他接收的所有消息和他自己的消息结合起来，形成组合消息，并在将其发送给下一层次之前，对该组合消息进行数字签名。在分层组织的最简单形式中，只有一个消息路由器，该路由器收集来自于所有其它交易参加者的消息，并把组合消息发送给 SP.

在串联组织中，交易的发起者与路由器和/或交易参加者串联，路由器和/或交易参加者再与服务提供商 60 串联。在本发明的一个优选实施例中，图 12 中所示的每个成分是一个交易参加者。在本发明的备选实施例中，交易发起者和 SP 之间的任何中间成分可以是路由器。

交易发起者与如图 12 中所示的串联排列的交易参加者 1100，1120，1140 和 1160，以及服务提供商执行交易。这类似于在图 6A-6Q 中描述的三方方案，只是现在所涉及的交易方更多。注意交易参加者 3，4，5，6… n-2 是以串联方式排列的。每个交易参加者准备好他自己的消息，把他自己的消息和从在前的交易参加者（如果有的话）收到的消息合并，对合并后的消息附加数字签名，随后将其发送给串联路径上的下一交易参加者。组合消息最终被发送给 SP，SP 据此形成响应消息，并通过初始的请求消息经过的同一路径回送响应消息。

图 13 表示了层次组织方案中布置的成分，这里每个成分 $X_{1,1}$ 到 $X_{1,n}$（n=1，2，3…）1200 是一个交易参加者，而不是消息路由器，每个成分 $X_{j,k}$（j=2，3，4，…；k=1，2，3，…，m；m 是 n 类型的变量；对于层次结构的不同层次来说，m 可以是不同的值）1210 可以交易参加者，也可以是路由器。向上的粗体箭头代表发送请求消息 1220。向下的箭头代表发送响应消息 1230。

每个交易参加者收集来自于他所负责的多个参加者的消息，并在把收集的消息和他自己的消息合并，形成新的消息之后，把该新消息发送给下一层次。层次组织方案可以只包括一个交易参加者，也可包括所需的尽可能多的交易参加者（层次方案的最简化的情况是一个交易参加者和一个服务提供商）。最后，在服务提供商之前的最后一个成分 $X_{\sigma,1}$ 处，所有消息被组合成一个消息 1240，σ是一个类型 n，该消息 1240 随后被发送给 SP 60。同样，SP 形成响应消息，并通过相同的路线回送该响应消息。

在 SP 不主导交易的情况下，会员使用由 SP 产生的对话密钥，在他们自己之间进行交易。交易可在两个或多个会员之间发生。当交易中涉及的会员多于两个时，消息可以任何顺序从一个会员传至另一会

员。会员发送交易请求消息，并接收交易响应消息。会员不必从他向其发送交易请求消息的同一会员那里接收交易响应消息。例如，交易中的三个会员可被组织成环形，并围绕该环发送消息。甲会员可向乙会员发送交易请求消息，乙会员再向丙会员发送交易请求消息和交易响应消息。丙会员向甲会员发送交易请求消息和交易响应消息，甲会员再向乙会员发送交易响应消息。接收交易请求消息的会员产生交易响应消息，该交易响应消息最终将被发送给发出交易请求消息的会员。

在密钥交换阶段，SP 获得所有参加交易会员的公共密钥。在交易参加会员在他们之间进行交易之前，SP 向每个交易参加会员发送其它会员的公共密钥。交易请求消息和交易响应消息包括明文（如果有的话），密码和发送方的数字签名。

在当 SP 需要充当 EC 和/或商家的凭证代理人，以便和基于凭证的外界系统打交道的情况下，SP 使 EC 和/或商家与外界接口的操作隔绝。SP 只向 EC 和/或商家返回完成与 EC 和/或商家的交易所需的信息。

虽然这里已描述了本发明的优选和例证实施例，不过对于本领域中的普通技术人员来说，本发明的其它修改将是显而易见的。于是，需要在附加权利要求中保护落入本发明的精神和范围内的所有这种修改和延伸。本发明将被解释为包括落入附加权利要求的范围内的本发明的所有实施例，并且本发明只应由下面的权利要求限定。另外，本领域中的普通技术人员将理解在不脱离本发明的精神和范围的情况下，其它应用可用于代替这里陈述的那些应用。

说 明 书 附 图

图1

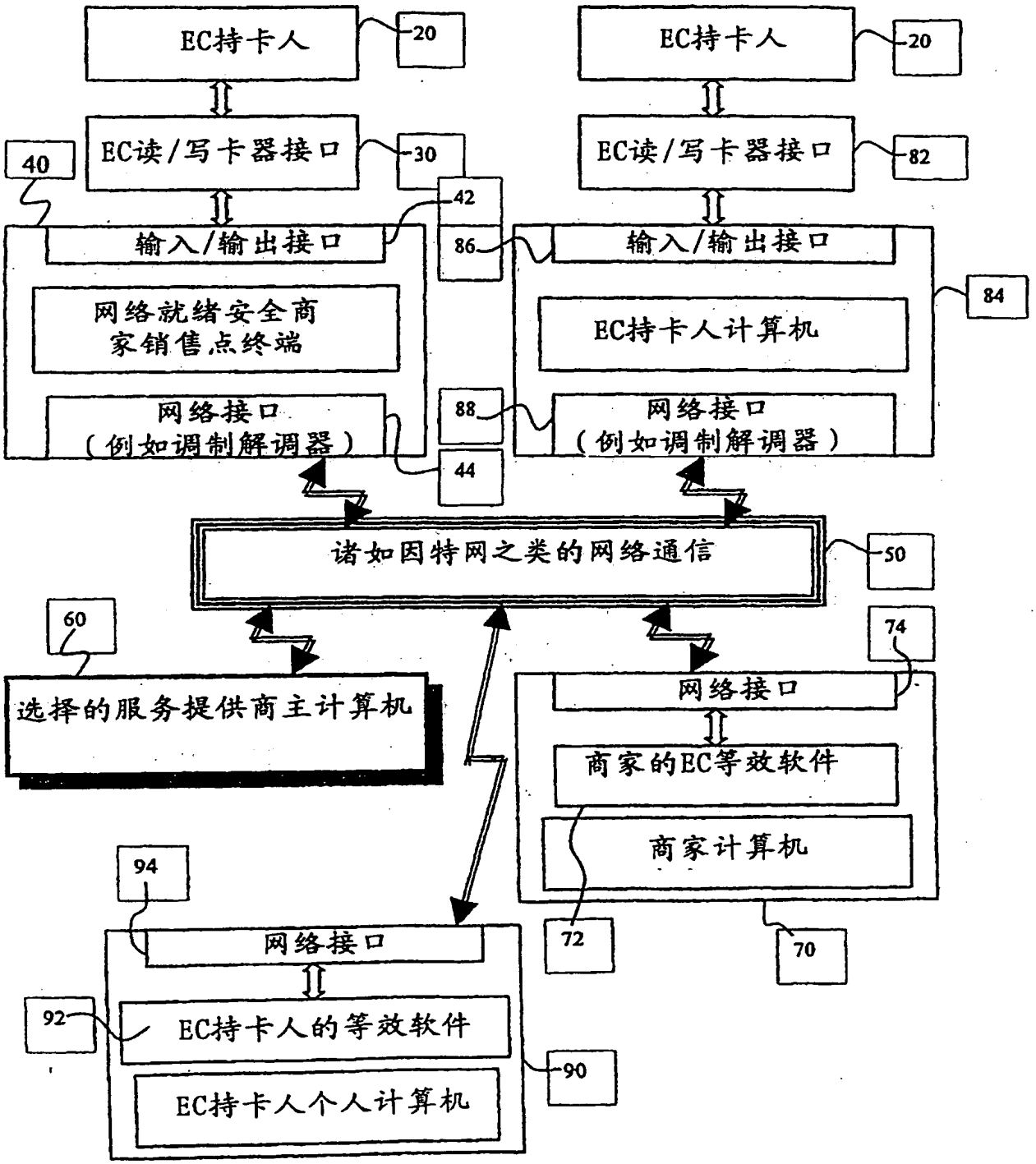

EC持卡人
20
EC持卡人
20
EC读/写卡器接口
30
EC读/写卡器接口
82
40
42
输入/输出接口
86
输入/输出接口
84
网络就绪安全商
家销售点终端
EC持卡人计算机
网络接口
（例如调制解调器）
88
网络接口
（例如调制解调器）
44
诸如因特网之类的网络通信
50
60
74
选择的服务提供商主计算机
网络接口
商家的EC等效软件
商家计算机
94
网络接口
72
70
92
EC持卡人的等效软件
90
EC持卡人个人计算机

图 2

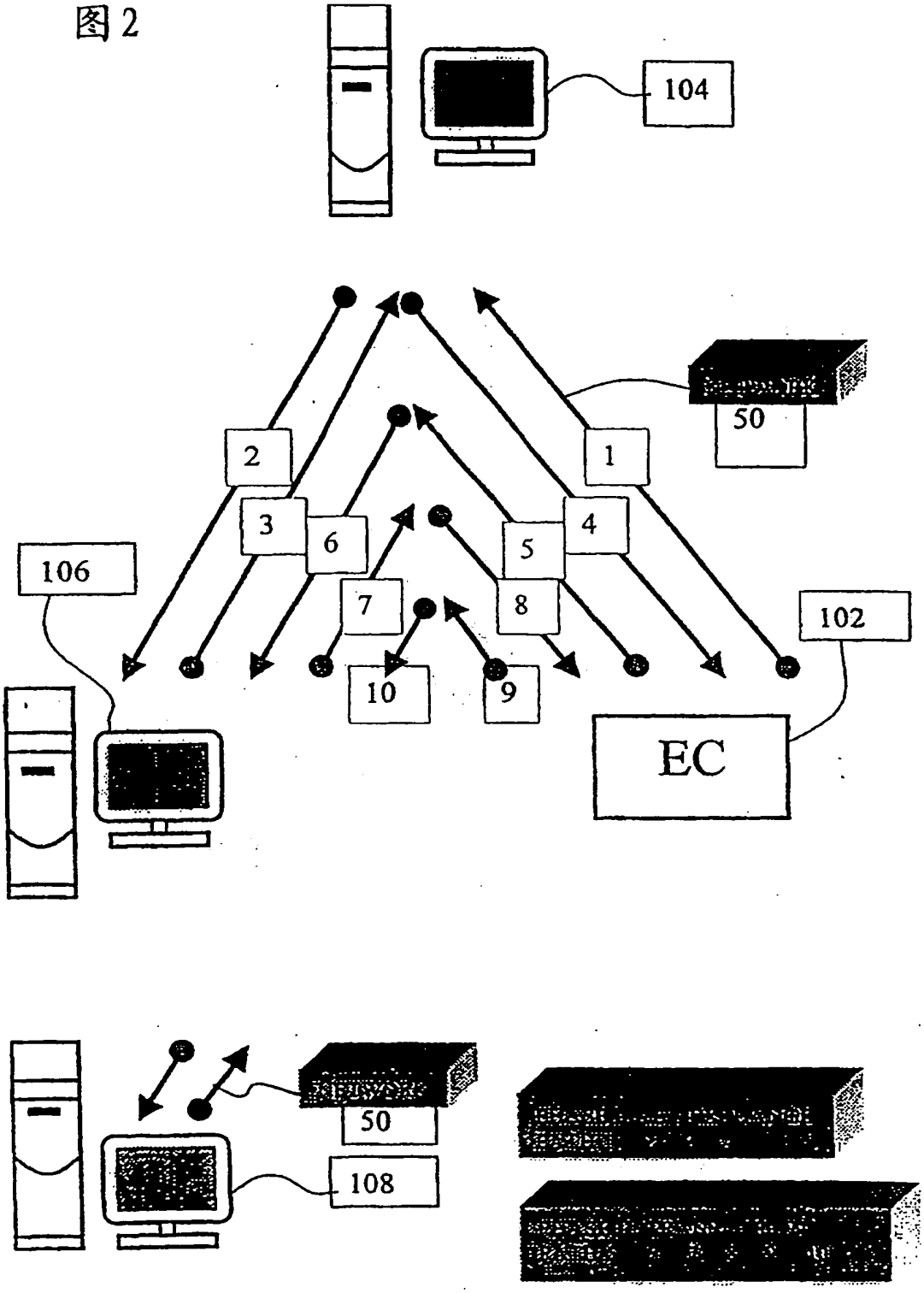
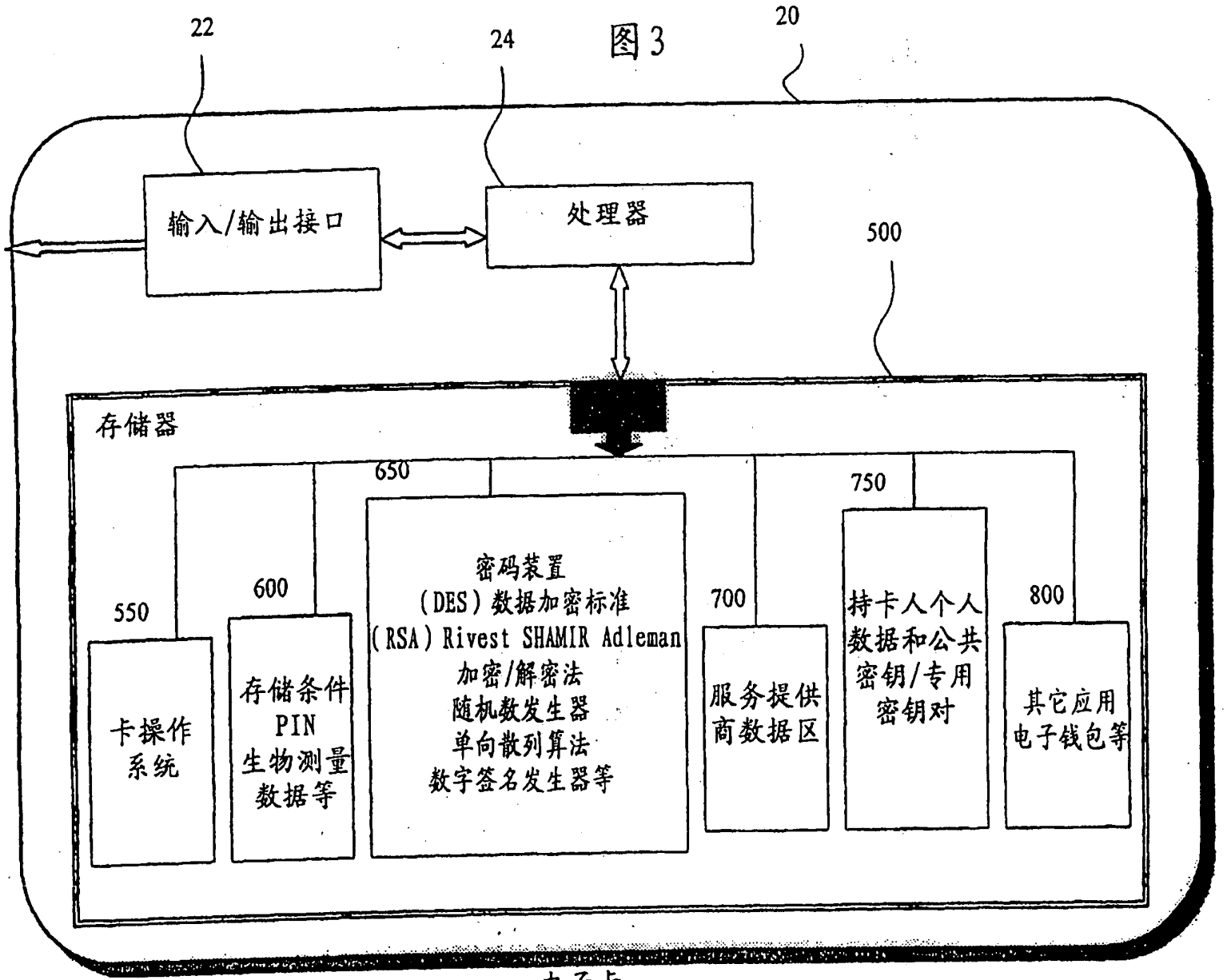


图3


22
24
20
输入/输出接口
处理器
500
存储器
650
750
密码装置
(DES)数据加密标准
(RSA) Rivest SHAMIR Adleman
加密/解密法
随机数发生器
单向散列算法
数字签名发生器等
550
600
700
800
卡操作系统
存储条件
PIN
生物测量数据等
服务提供商数据区
持卡人个人数据和公共密钥/专用密钥对
其它应用电子钱包等
电子卡

700

图4

服务提供商数据区（SPDA）						
702	704	706	708	710	712	714
名称	密钥类型	密钥值	（帐号信息）（帐号，终止日期等）	卡类型	PIN（可选）	杂项数据
				信用卡		
				借记卡		
				ATM卡		
				会员卡		
				LOYALTY卡		
				等		

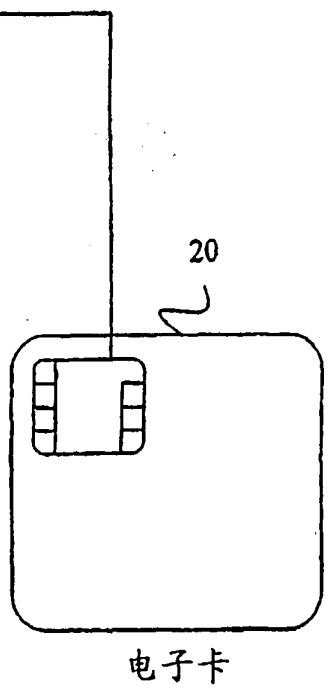


图 5

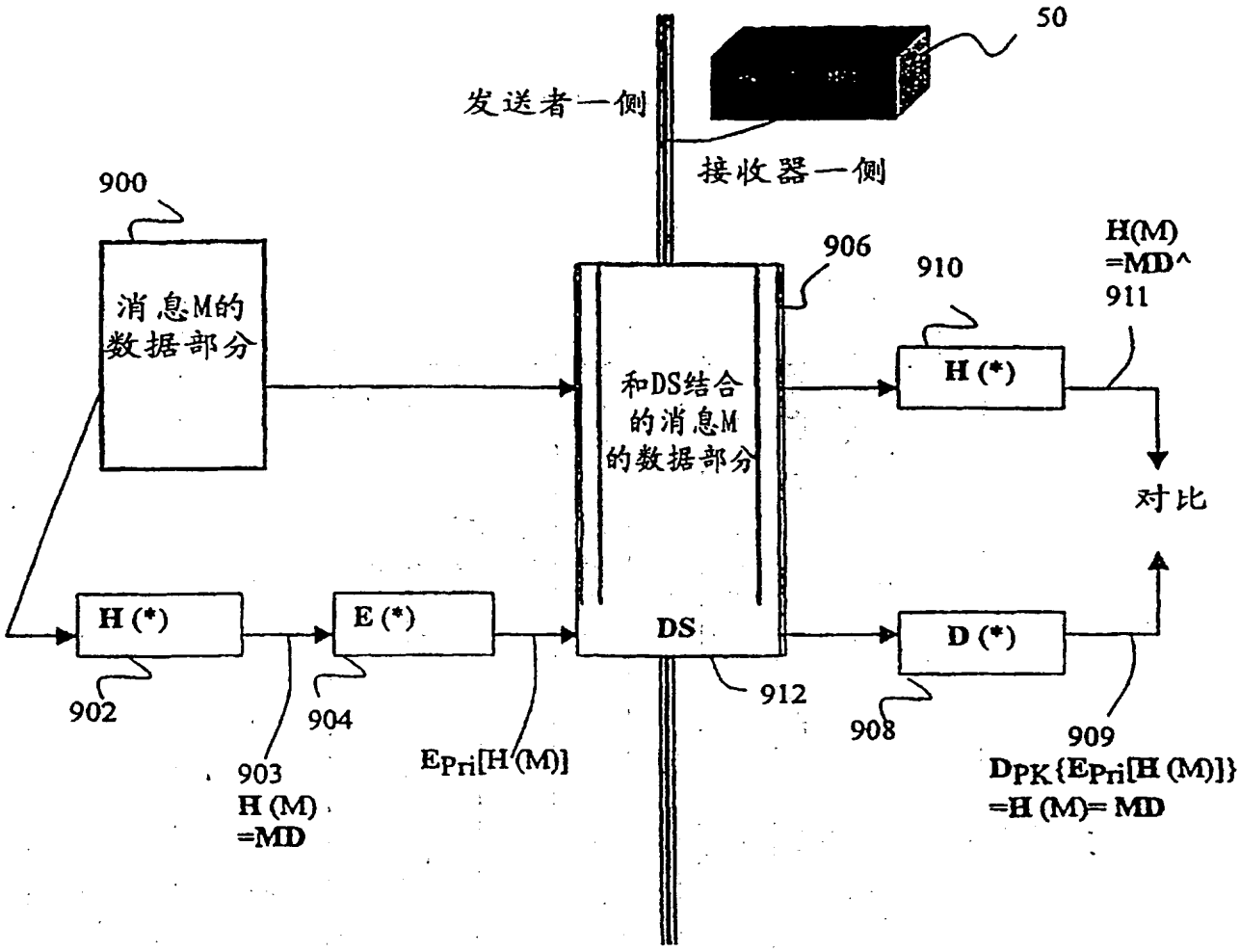

50
发送者一侧
接收器一侧
900
消息M的数据部分
906
910
H(M)
=MD^
911
和DS结合的消息M的数据部分
H (*)
对比
H (*)
E (*)
DS
D (*)
902
904
912
908
909
903
H (M)
=MD
EPri[H (M)]
DPK{EPri[H (M)]}
=H (M)= MD

图6A

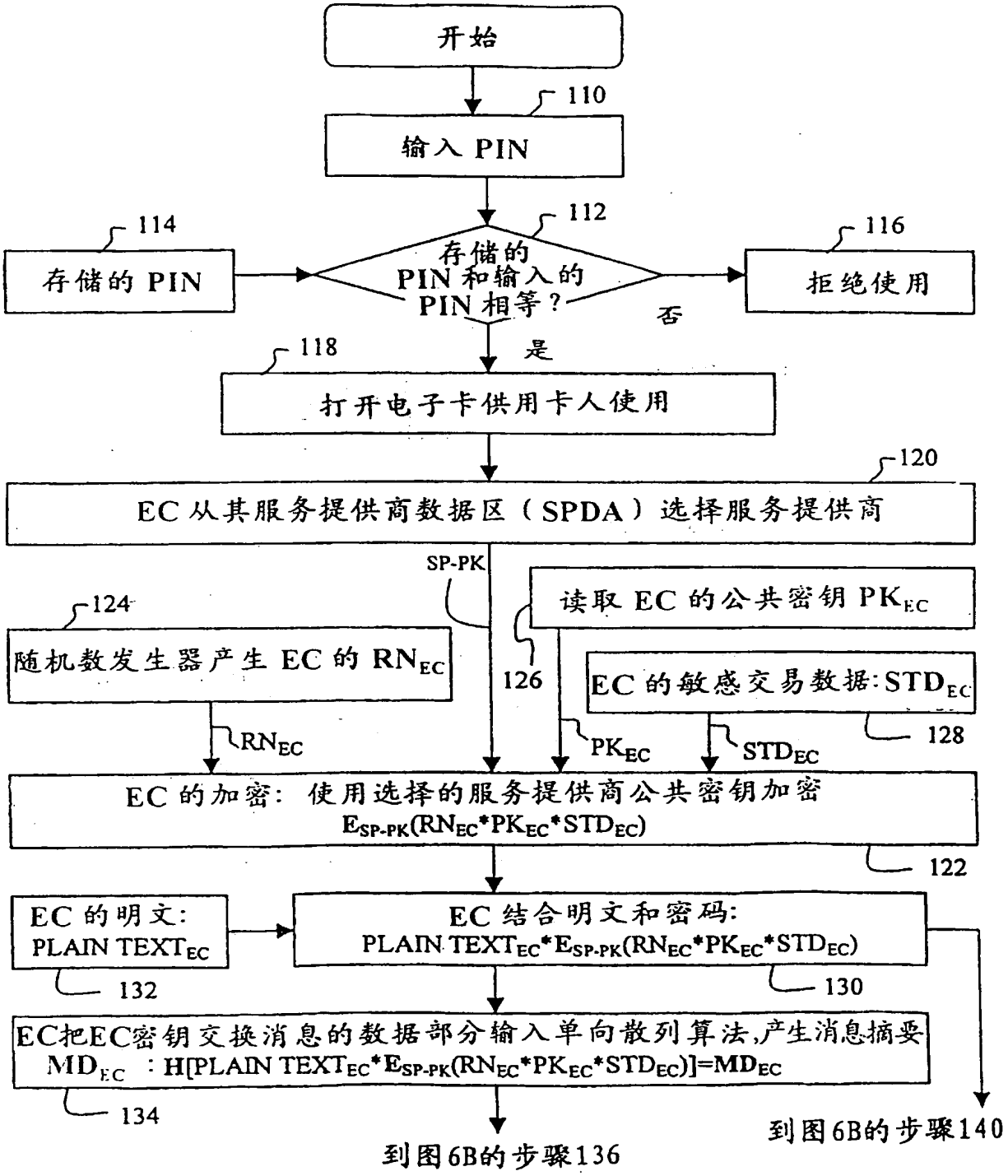

开始
110
输入 PIN
112
114
存储的 PIN
存储的 PIN 和输入的 PIN 相等？
否
116
拒绝使用
是
118
打开电子卡供用卡人使用
120
EC 从其服务提供商数据区（SPDA）选择服务提供商
SP-PK
读取 EC 的公共密钥 PK_{EC}
124
随机数发生器产生 EC 的 RN_{EC}
126
EC 的敏感交易数据: STD_{EC}
128
RN_{EC}
PK_{EC}
STD_{EC}
EC 的加密：使用选择的服务提供商公共密钥加密
$E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})$
122
EC 的明文:
PLAIN $TEXT_{EC}$
EC 结合明文和密码:
PLAIN $TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})$
132
130
EC把EC密钥交换消息的数据部分输入单向散列算法,产生消息摘要
MD_{EC} : $H[PLAIN\ TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]=MD_{EC}$
134
到图6B的步骤136
到图6B的步骤140

图*6B*

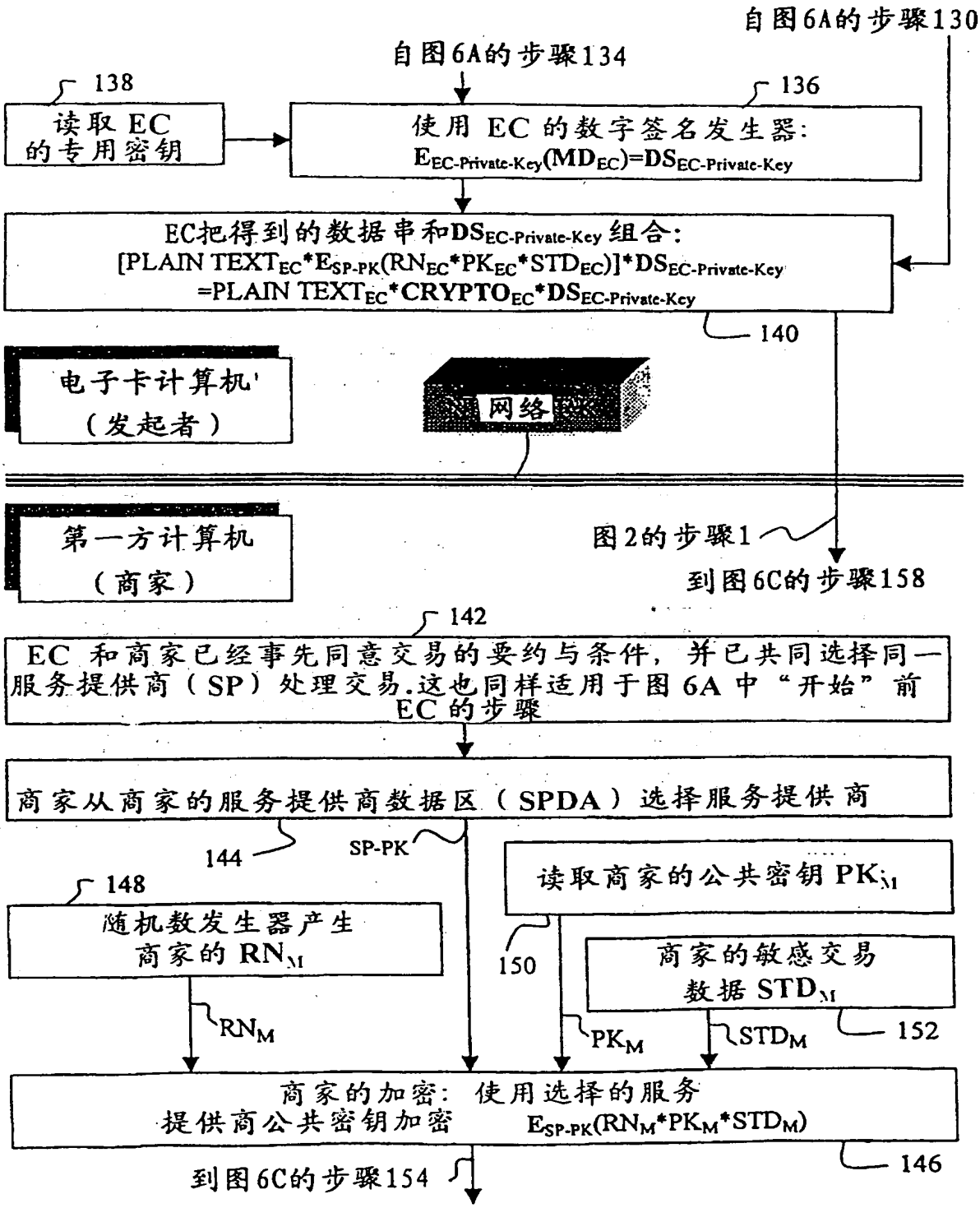

自图6A的步骤130
自图6A的步骤134
138
读取 EC 的专用密钥
136
使用 EC 的数字签名发生器:
$E_{EC\text{-}Private\text{-}Key}(MD_{EC})=DS_{EC\text{-}Private\text{-}Key}$
EC把得到的数据串和$DS_{EC\text{-}Private\text{-}Key}$组合:
$[PLAIN\ TEXT_{EC}*E_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})]*DS_{EC\text{-}Private\text{-}Key}$
$=PLAIN\ TEXT_{EC}*CRYPTO_{EC}*DS_{EC\text{-}Private\text{-}Key}$
140
电子卡计算机'
(发起者)
网络
第一方计算机
(商家)
图2的步骤1
到图6C的步骤158
142
EC 和商家已经事先同意交易的要约与条件，并已共同选择同一服务提供商（SP）处理交易.这也同样适用于图 6A 中“开始”前 EC 的步骤
商家从商家的服务提供商数据区（SPDA）选择服务提供商
144
SP-PK
读取商家的公共密钥 PK_M
148
随机数发生器产生商家的 RN_M
150
商家的敏感交易数据 STD_M
152
RN_M
PK_M
STD_M
商家的加密: 使用选择的服务提供商公共密钥加密 $E_{SP\text{-}PK}(RN_M*PK_M*STD_M)$
146
到图6C的步骤154

图6C

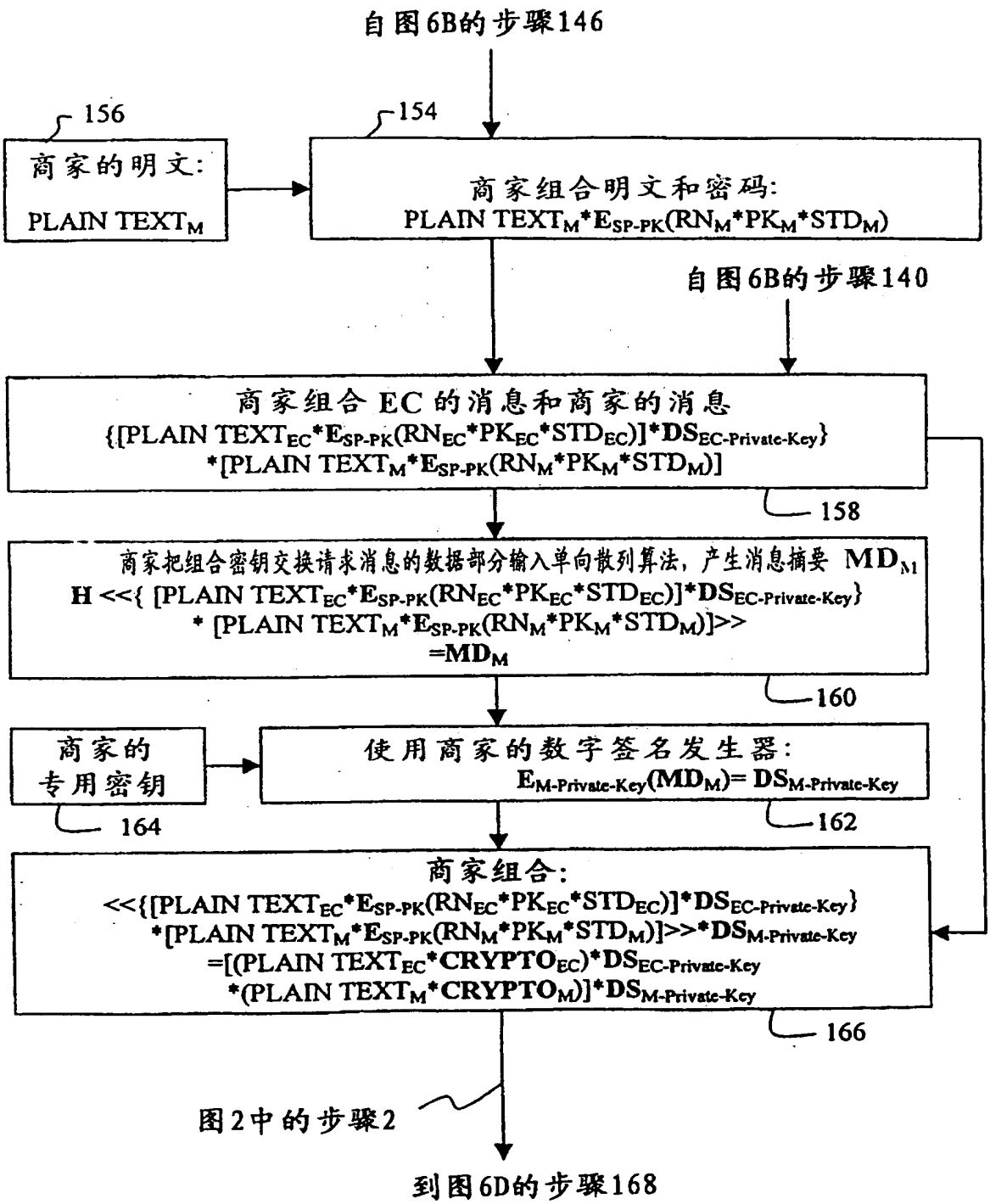

自图6B的步骤146
156
154
商家的明文:
PLAIN TEXT$_M$
商家组合明文和密码:
PLAIN TEXT$_M$*E$_{SP-PK}$(RN$_M$*PK$_M$*STD$_M$)
自图6B的步骤140
商家组合EC的消息和商家的消息
{[PLAIN TEXT$_{EC}$*E$_{SP-PK}$(RN$_{EC}$*PK$_{EC}$*STD$_{EC}$)]*DS$_{EC-Private-Key}$}
*[PLAIN TEXT$_M$*E$_{SP-PK}$(RN$_M$*PK$_M$*STD$_M$)]
158
商家把组合密钥交换请求消息的数据部分输入单向散列算法，产生消息摘要 MD$_M$
H <<{ [PLAIN TEXT$_{EC}$*E$_{SP-PK}$(RN$_{EC}$*PK$_{EC}$*STD$_{EC}$)]*DS$_{EC-Private-Key}$}
* [PLAIN TEXT$_M$*E$_{SP-PK}$(RN$_M$*PK$_M$*STD$_M$)]>>
=MD$_M$
160
商家的
专用密钥
使用商家的数字签名发生器:
E$_{M-Private-Key}$(MD$_M$)= DS$_{M-Private-Key}$
164
162
商家组合:
<<{[PLAIN TEXT$_{EC}$*E$_{SP-PK}$(RN$_{EC}$*PK$_{EC}$*STD$_{EC}$)]*DS$_{EC-Private-Key}$}
*[PLAIN TEXT$_M$*E$_{SP-PK}$(RN$_M$*PK$_M$*STD$_M$)]>>*DS$_{M-Private-Key}$
=[(PLAIN TEXT$_{EC}$*CRYPTO$_{EC}$)*DS$_{EC-Private-Key}$
*(PLAIN TEXT$_M$*CRYPTO$_M$)]*DS$_{M-Private-Key}$
166
图2中的步骤2
到图6D的步骤168

图6D

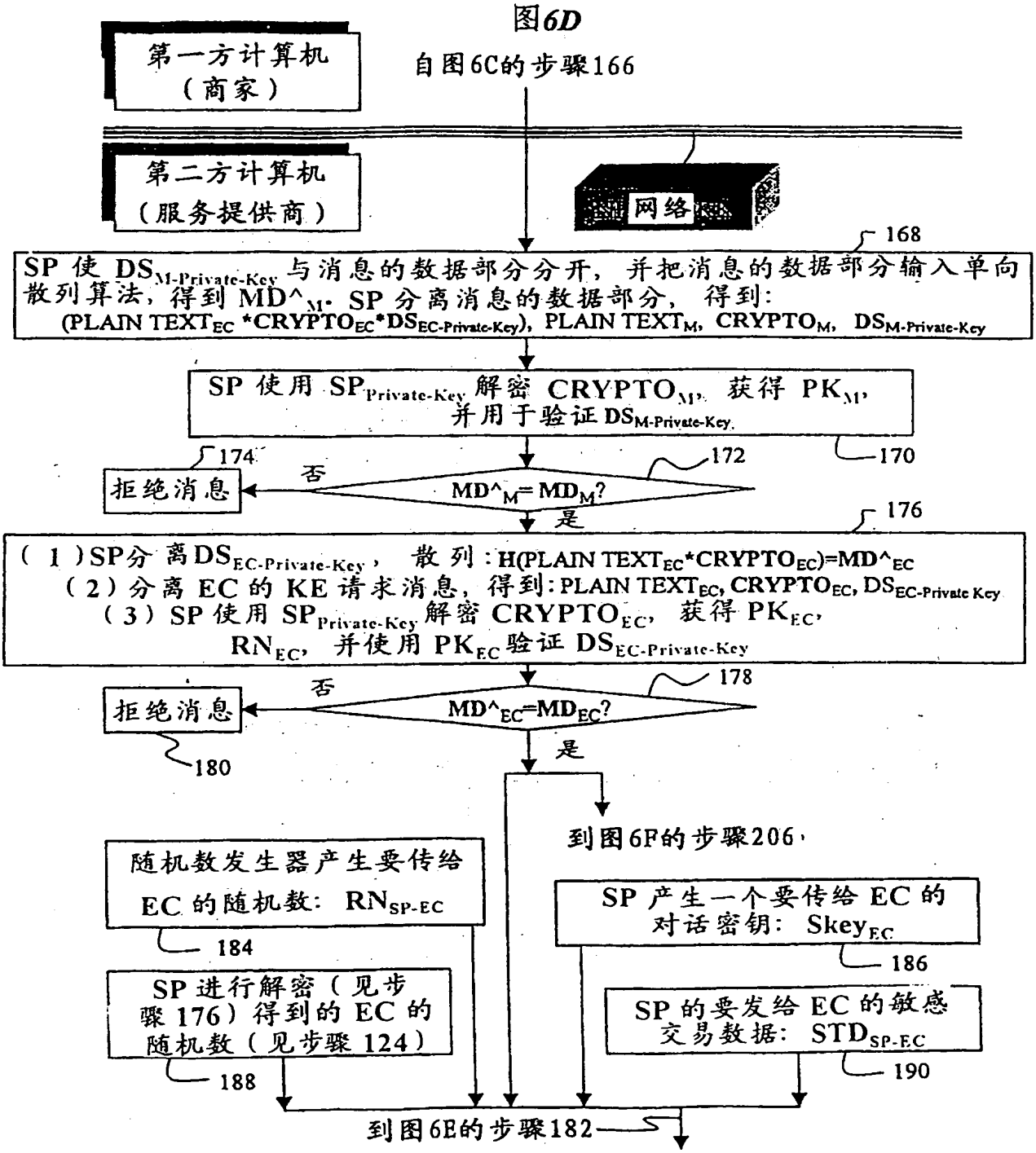
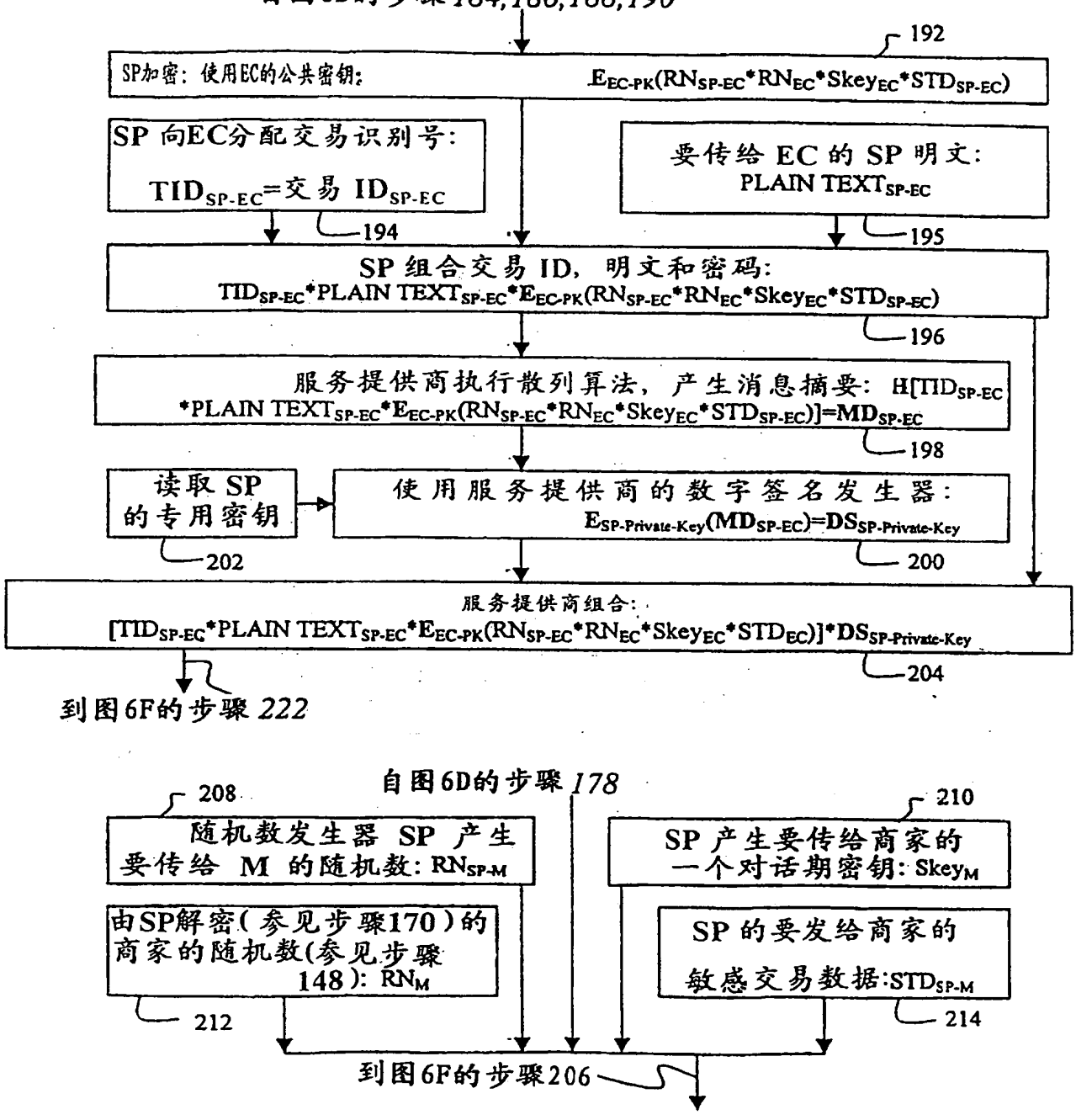

第一方计算机
（商家）
自图6C的步骤166
第二方计算机
（服务提供商）
网络
168
SP 使 $DS_{M\text{-}Private\text{-}Key}$ 与消息的数据部分分开，并把消息的数据部分输入单向散列算法，得到 $MD^{\wedge}_{M}$. SP 分离消息的数据部分，得到：
$(PLAIN\ TEXT_{EC}*CRYPTO_{EC}*DS_{EC\text{-}Private\text{-}Key})$, $PLAIN\ TEXT_{M}$, $CRYPTO_{M}$, $DS_{M\text{-}Private\text{-}Key}$
SP 使用 $SP_{Private\text{-}Key}$ 解密 $CRYPTO_{M}$，获得 PK_{M}，并用于验证 $DS_{M\text{-}Private\text{-}Key}$.
170
174
拒绝消息
否
172
$MD^{\wedge}_{M}=MD_{M}$?
是
176
（1）SP分离 $DS_{EC\text{-}Private\text{-}Key}$，散列：$H(PLAIN\ TEXT_{EC}*CRYPTO_{EC})=MD^{\wedge}_{EC}$
（2）分离 EC 的 KE 请求消息，得到：$PLAIN\ TEXT_{EC}$, $CRYPTO_{EC}$, $DS_{EC\text{-}Private\ Key}$
（3）SP 使用 $SP_{Private\text{-}Key}$ 解密 $CRYPTO_{EC}$，获得 PK_{EC}，RN_{EC}，并使用 PK_{EC} 验证 $DS_{EC\text{-}Private\text{-}Key}$
178
拒绝消息
否
$MD^{\wedge}_{EC}=MD_{EC}$?
是
180
到图6F的步骤206，
随机数发生器产生要传给 EC 的随机数：$RN_{SP\text{-}EC}$
184
SP 产生一个要传给 EC 的对话密钥：$Skey_{EC}$
186
SP 进行解密（见步骤 176）得到的 EC 的随机数（见步骤 124）
188
SP 的要发给 EC 的敏感交易数据：$STD_{SP\text{-}EC}$
190
到图6E的步骤182

图 6E


自图6D的步骤 184,186,188,190
192
SP加密：使用EC的公共密钥：
$E_{EC-PK}(RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{SP-EC})$
SP 向EC分配交易识别号：
TID_{SP-EC}=交易 ID_{SP-EC}
194
要传给 EC 的 SP 明文：
$PLAIN\ TEXT_{SP-EC}$
195
SP 组合交易 ID，明文和密码：
$TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*E_{EC-PK}(RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{SP-EC})$
196
服务提供商执行散列算法，产生消息摘要：$H[TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*E_{EC-PK}(RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{SP-EC})]=MD_{SP-EC}$
198
读取 SP 的专用密钥
202
使用服务提供商的数字签名发生器：
$E_{SP-Private-Key}(MD_{SP-EC})=DS_{SP-Private-Key}$
200
服务提供商组合：
$[TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*E_{EC-PK}(RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{EC})]*DS_{SP-Private-Key}$
204
到图6F的步骤 222

自图6D的步骤 178
208
随机数发生器 SP 产生要传给 M 的随机数：RN_{SP-M}
210
SP 产生要传给商家的一个对话期密钥：$Skey_M$
由SP解密（参见步骤170）的商家的随机数(参见步骤148)：RN_M
212
SP 的要发给商家的敏感交易数据：STD_{SP-M}
214
到图6F的步骤206

图 6F

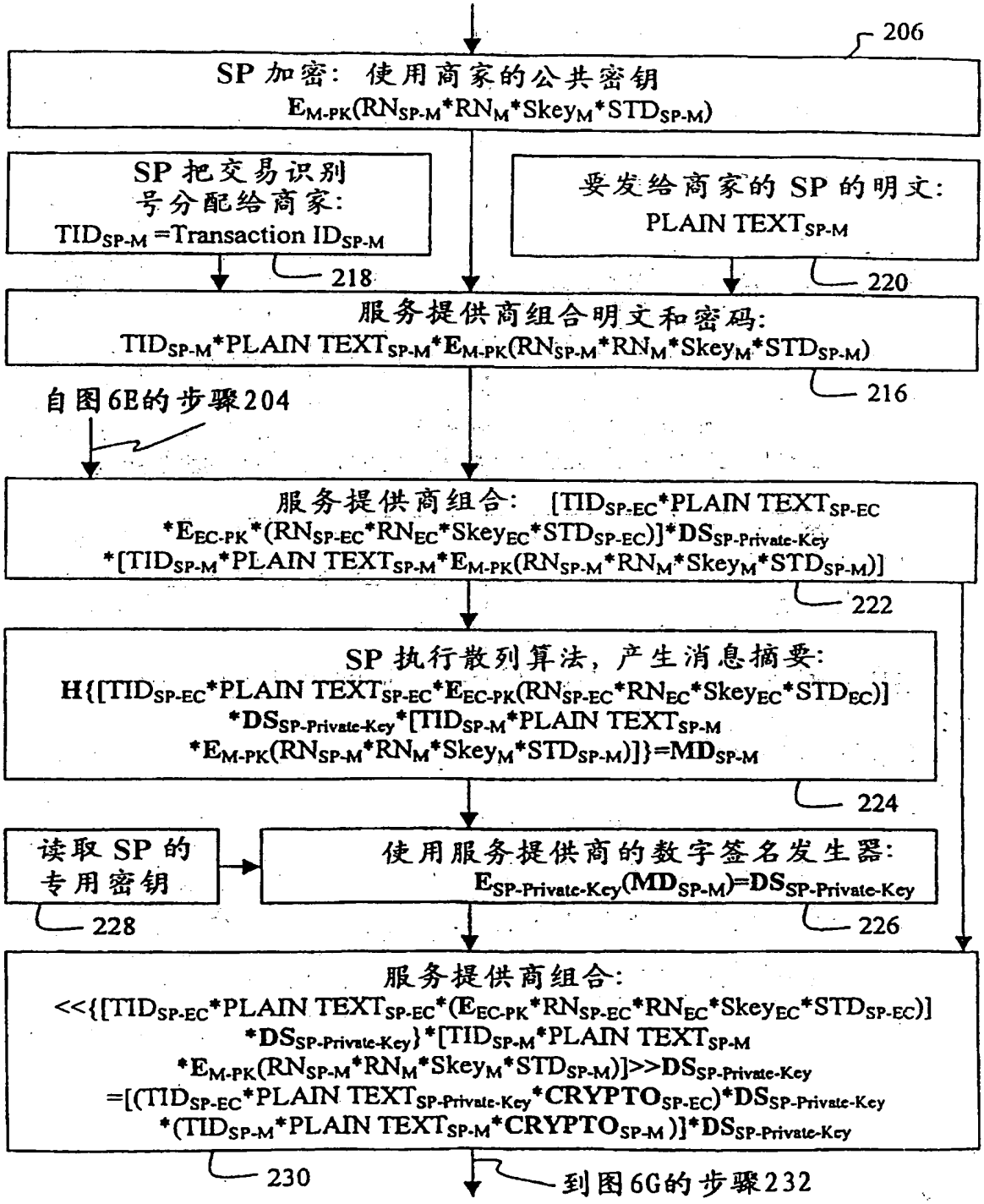

自图6E的步骤 208,210, 212,214
206
SP 加密：使用商家的公共密钥
$E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})$
SP 把交易识别号分配给商家:
$TID_{SP\text{-}M}$ =Transaction $ID_{SP\text{-}M}$
218
要发给商家的 SP 的明文:
$PLAIN\ TEXT_{SP\text{-}M}$
220
服务提供商组合明文和密码:
$TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})$
216
自图6E的步骤204
服务提供商组合: $[TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*E_{EC\text{-}PK}*(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]*DS_{SP\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]$
222
SP 执行散列算法，产生消息摘要:
$H\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*E_{EC\text{-}PK}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{EC})]*DS_{SP\text{-}Private\text{-}Key}*[TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]\}=MD_{SP\text{-}M}$
224
读取 SP 的专用密钥
228
使用服务提供商的数字签名发生器:
$E_{SP\text{-}Private\text{-}Key}(MD_{SP\text{-}M})=DS_{SP\text{-}Private\text{-}Key}$
226
服务提供商组合:
$<<\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*(E_{EC\text{-}PK}*RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]*DS_{SP\text{-}Private\text{-}Key}\}*[TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*E_{M\text{-}PK}(RN_{SP\text{-}M}*RN_M*Skey_M*STD_{SP\text{-}M})]>>DS_{SP\text{-}Private\text{-}Key}=[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}Private\text{-}Key}*CRYPTO_{SP\text{-}EC})*DS_{SP\text{-}Private\text{-}Key}*(TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*CRYPTO_{SP\text{-}M})]*DS_{SP\text{-}Private\text{-}Key}$
230
到图6G的步骤232

图6G

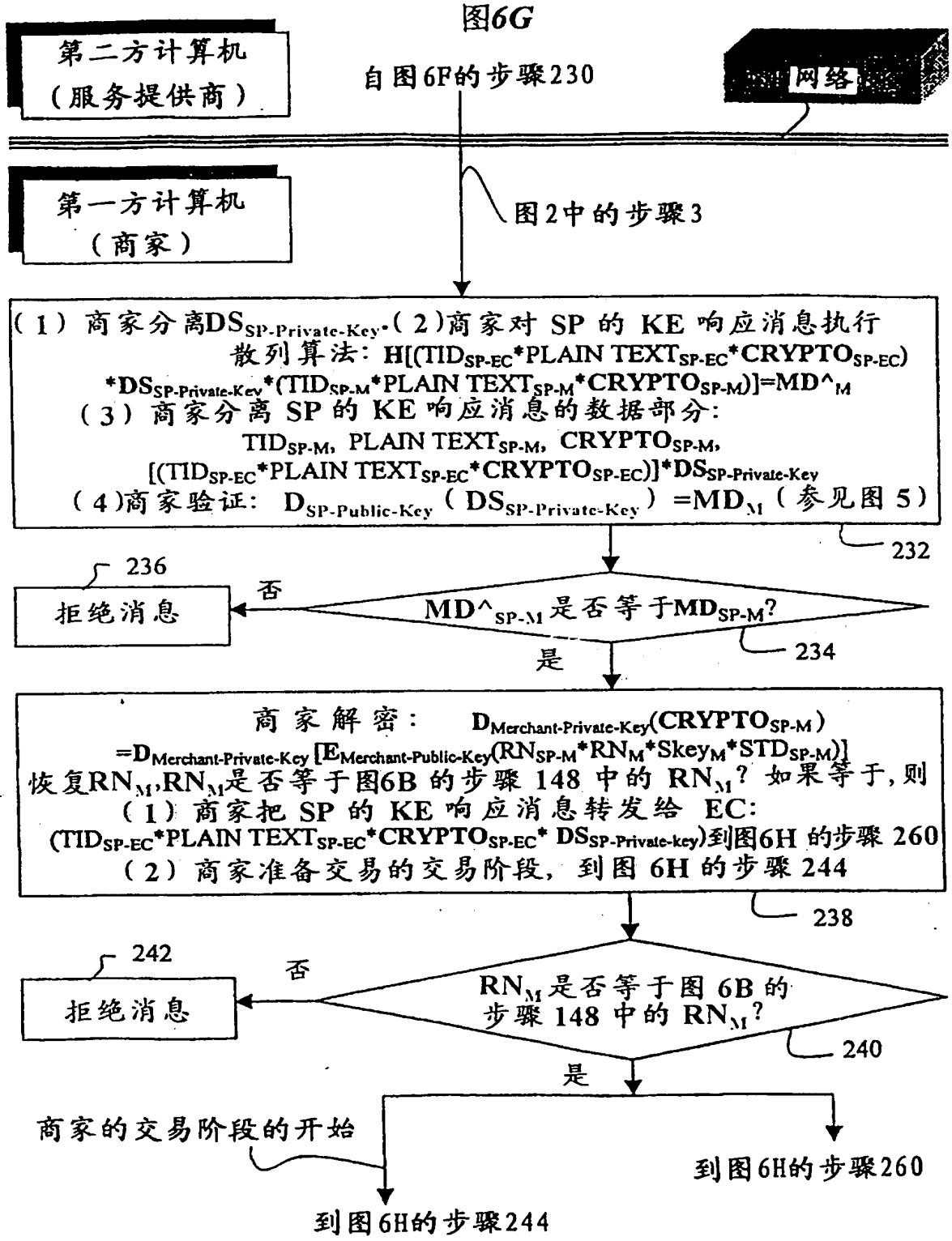

第二方计算机
（服务提供商）
自图6F的步骤230
网络
第一方计算机
（商家）
图2中的步骤3
（1）商家分离$DS_{SP\text{-}Private\text{-}Key}$·（2）商家对 SP 的 KE 响应消息执行散列算法：$H[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*CRYPTO_{SP\text{-}EC})*DS_{SP\text{-}Private\text{-}Key}*(TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*CRYPTO_{SP\text{-}M})]=MD^{\wedge}_{M}$
（3）商家分离 SP 的 KE 响应消息的数据部分：
$TID_{SP\text{-}M}$, $PLAIN\ TEXT_{SP\text{-}M}$, $CRYPTO_{SP\text{-}M}$,
$[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*CRYPTO_{SP\text{-}EC})]*DS_{SP\text{-}Private\text{-}Key}$
（4）商家验证：$D_{SP\text{-}Public\text{-}Key}(DS_{SP\text{-}Private\text{-}Key})=MD_{M}$（参见图 5）
232
$MD^{\wedge}_{SP\text{-}M}$是否等于$MD_{SP\text{-}M}$?
234
否
236
拒绝消息
是
商家解密：$D_{Merchant\text{-}Private\text{-}Key}(CRYPTO_{SP\text{-}M})=D_{Merchant\text{-}Private\text{-}Key}[E_{Merchant\text{-}Public\text{-}Key}(RN_{SP\text{-}M}*RN_{M}*Skey_{M}*STD_{SP\text{-}M})]$
恢复RN_{M},RN_{M}是否等于图6B 的步骤 148 中的 RN_{M}？如果等于，则
（1）商家把 SP 的 KE 响应消息转发给 EC：
$(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*CRYPTO_{SP\text{-}EC}*DS_{SP\text{-}Private\text{-}key})$到图6H 的步骤 260
（2）商家准备交易的交易阶段，到图 6H 的步骤 244
238
RN_{M}是否等于图 6B 的步骤 148 中的 RN_{M}?
240
否
242
拒绝消息
是
商家的交易阶段的开始
到图6H的步骤260
到图6H的步骤244

图 6H

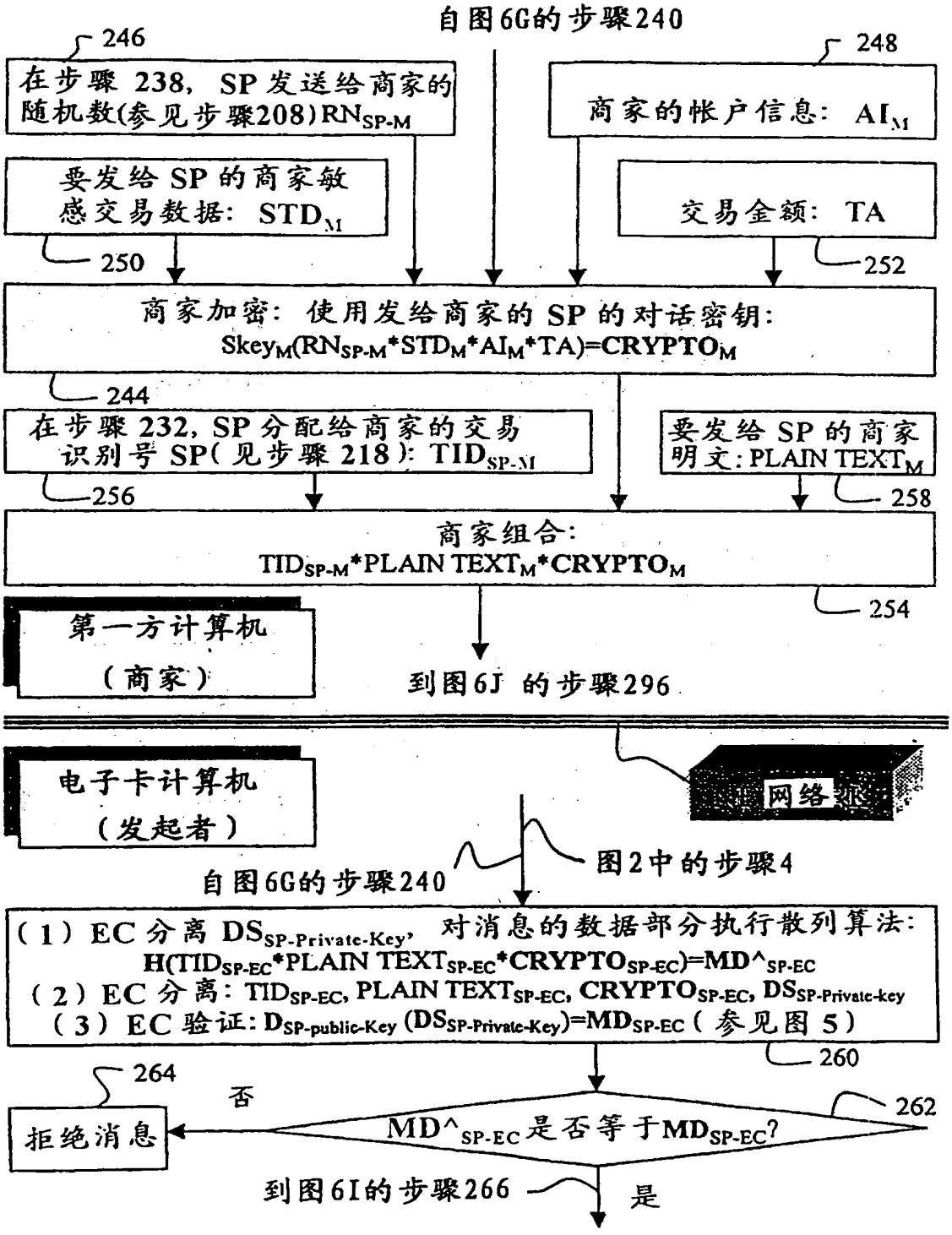
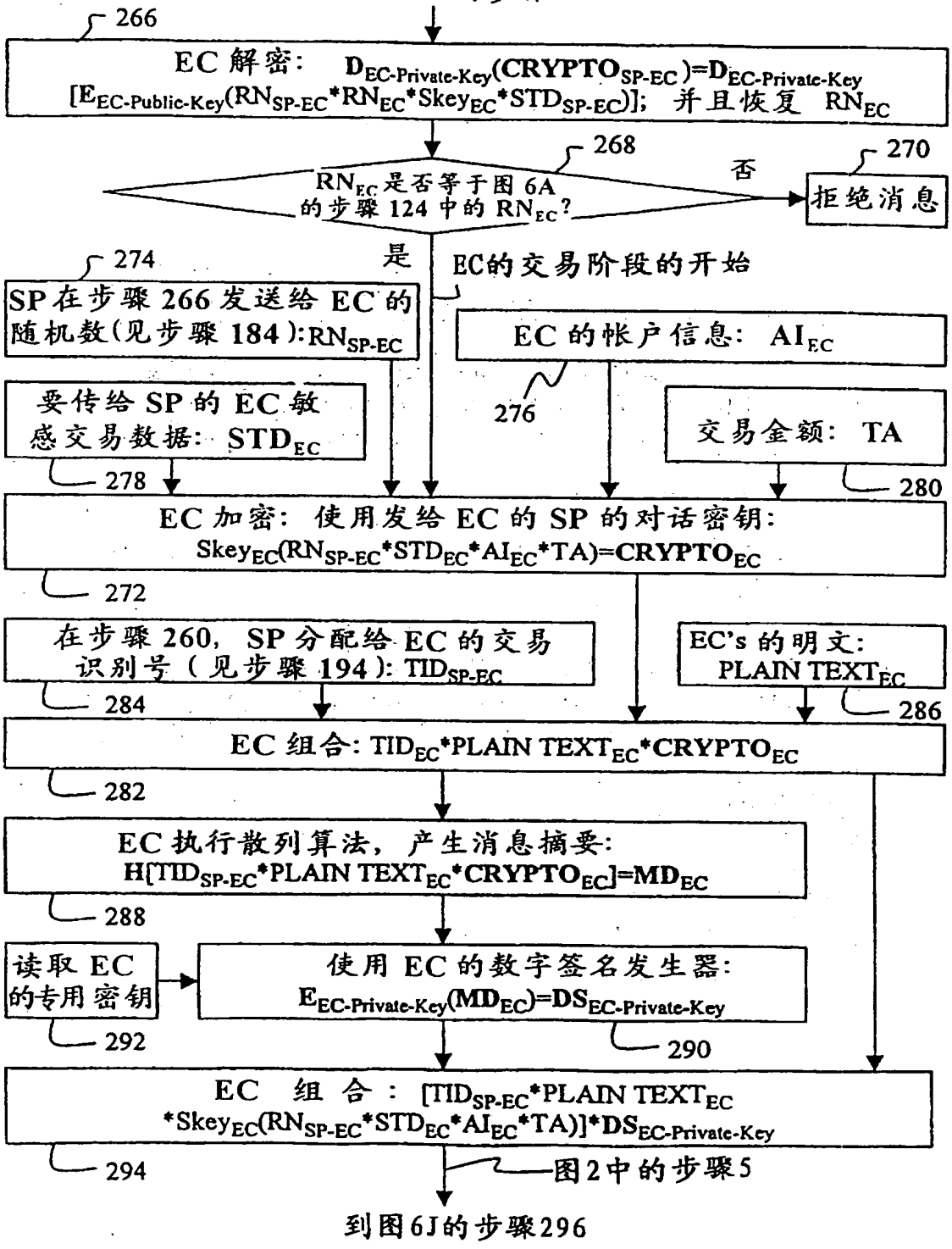

自图6G的步骤240
246
在步骤 238，SP 发送给商家的随机数(参见步骤208) RN_{SP-M}
248
商家的帐户信息：AI_M
要发给 SP 的商家敏感交易数据：STD_M
交易金额：TA
250
252
商家加密：使用发给商家的 SP 的对话密钥：
$Skey_M(RN_{SP-M}*STD_M*AI_M*TA)=CRYPTO_M$
244
在步骤 232，SP 分配给商家的交易识别号 SP（见步骤 218）：TID_{SP-M}
要发给 SP 的商家明文：$PLAIN\ TEXT_M$
256
258
商家组合：
$TID_{SP-M}*PLAIN\ TEXT_M*CRYPTO_M$
254
第一方计算机
（商家）
到图6J 的步骤296
网络
电子卡计算机
（发起者）
图2中的步骤4
自图6G的步骤240
（1）EC 分离 $DS_{SP-Private-Key}$，对消息的数据部分执行散列算法：
$H(TID_{SP-EC}*PLAIN\ TEXT_{SP-EC}*CRYPTO_{SP-EC})=MD^{\wedge}_{SP-EC}$
（2）EC 分离：TID_{SP-EC}, $PLAIN\ TEXT_{SP-EC}$, $CRYPTO_{SP-EC}$, $DS_{SP-Private-key}$
（3）EC 验证：$D_{SP-public-Key}(DS_{SP-Private-Key})=MD_{SP-EC}$（参见图 5）
260
264
否
262
拒绝消息
$MD^{\wedge}_{SP-EC}$ 是否等于 MD_{SP-EC}?
到图6I的步骤266
是

图6I


自图6H的步骤262
266
EC 解密: $D_{EC\text{-}Private\text{-}Key}(CRYPTO_{SP\text{-}EC})=D_{EC\text{-}Private\text{-}Key}[E_{EC\text{-}Public\text{-}Key}(RN_{SP\text{-}EC}*RN_{EC}*Skey_{EC}*STD_{SP\text{-}EC})]$; 并且恢复 RN_{EC}
268
RN_{EC}是否等于图6A的步骤124中的RN_{EC}?
否
270
拒绝消息
是
EC的交易阶段的开始
274
SP在步骤266发送给EC的随机数(见步骤184):$RN_{SP\text{-}EC}$
EC 的帐户信息: AI_{EC}
276
要传给SP的EC敏感交易数据: STD_{EC}
交易金额: TA
278
280
EC 加密: 使用发给EC的SP的对话密钥: $Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)=CRYPTO_{EC}$
272
在步骤260, SP分配给EC的交易识别号(见步骤194): $TID_{SP\text{-}EC}$
EC's 的明文: $PLAIN\ TEXT_{EC}$
284
286
EC 组合: $TID_{EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC}$
282
EC 执行散列算法, 产生消息摘要: $H[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC}]=MD_{EC}$
288
读取EC的专用密钥
使用 EC 的数字签名发生器: $E_{EC\text{-}Private\text{-}Key}(MD_{EC})=DS_{EC\text{-}Private\text{-}Key}$
292
290
EC 组合: $[TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(RN_{SP\text{-}EC}*STD_{EC}*AI_{EC}*TA)]*DS_{EC\text{-}Private\text{-}Key}$
294
图2中的步骤5
到图6J的步骤296

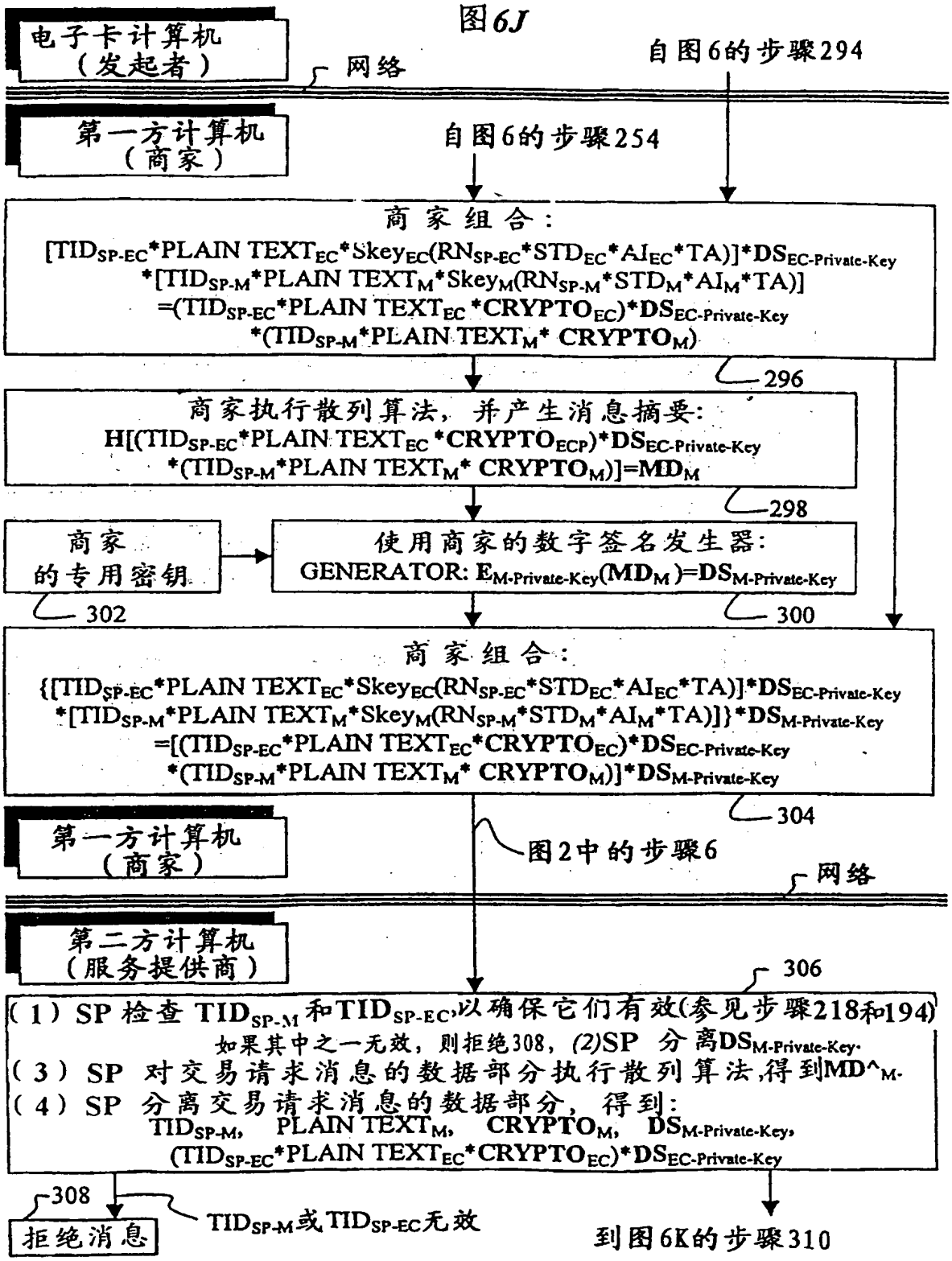


图6J
电子卡计算机（发起者）
网络
自图6的步骤294
第一方计算机（商家）
自图6的步骤254
商家组合：
[TIDSP-EC*PLAIN TEXTEC*SkeyEC(RNSP-EC*STDEC*AIEC*TA)]*DSEC-Private-Key
*[TIDSP-M*PLAIN TEXTM*SkeyM(RNSP-M*STDM*AIM*TA)]
=(TIDSP-EC*PLAIN TEXTEC*CRYPTOEC)*DSEC-Private-Key
*(TIDSP-M*PLAIN TEXTM* CRYPTOM)
296
商家执行散列算法，并产生消息摘要：
H[(TIDSP-EC*PLAIN TEXTEC*CRYPTOECP)*DSEC-Private-Key
*(TIDSP-M*PLAIN TEXTM* CRYPTOM)]=MDM
298
商家的专用密钥
使用商家的数字签名发生器：
GENERATOR: EM-Private-Key(MDM)=DSM-Private-Key
302
300
商家组合：
{[TIDSP-EC*PLAIN TEXTEC*SkeyEC(RNSP-EC*STDEC*AIEC*TA)]*DSEC-Private-Key
*[TIDSP-M*PLAIN TEXTM*SkeyM(RNSP-M*STDM*AIM*TA)]}*DSM-Private-Key
=[(TIDSP-EC*PLAIN TEXTEC*CRYPTOEC)*DSEC-Private-Key
*(TIDSP-M*PLAIN TEXTM* CRYPTOM)]*DSM-Private-Key
304
第一方计算机（商家）
图2中的步骤6
网络
第二方计算机（服务提供商）
306
(1) SP 检查 TIDSP-M和TIDSP-EC,以确保它们有效(参见步骤218和194)
如果其中之一无效，则拒绝308，(2)SP 分离DSM-Private-Key.
(3) SP 对交易请求消息的数据部分执行散列算法,得到MD^M.
(4) SP 分离交易请求消息的数据部分，得到：
TIDSP-M, PLAIN TEXTM, CRYPTOM, DSM-Private-Key,
(TIDSP-EC*PLAIN TEXTEC*CRYPTOEC)*DSEC-Private-Key
308
拒绝消息
TIDSP-M或TIDSP-EC无效
到图6K的步骤310

图6K

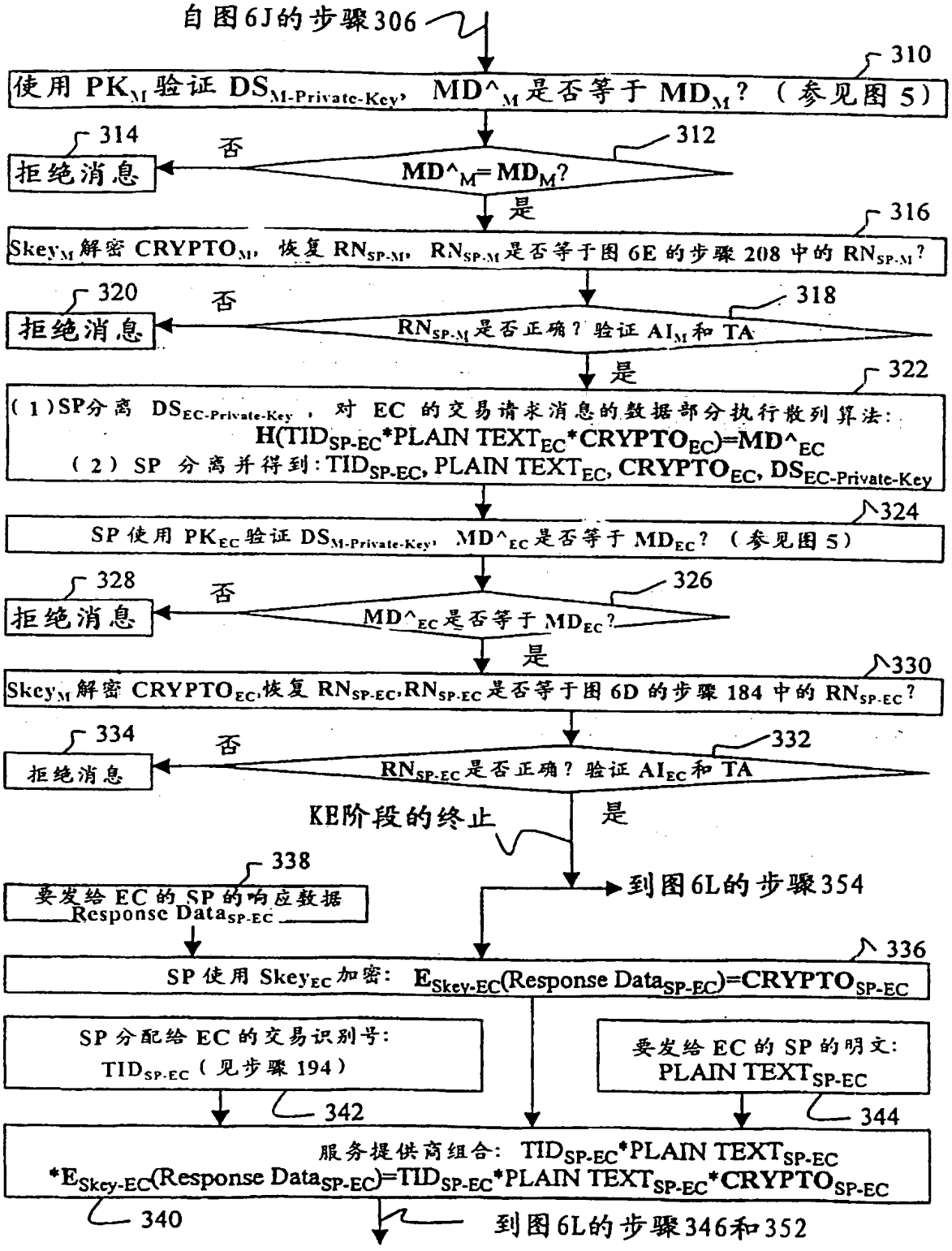

自图6J的步骤306
310
使用 PK_M 验证 $DS_{M\text{-}Private\text{-}Key}$，$MD^{\wedge}_M$ 是否等于 MD_M？（参见图5）
312
$MD^{\wedge}_M = MD_M$?
否
314
拒绝消息
是
316
$Skey_M$ 解密 $CRYPTO_M$，恢复 $RN_{SP\text{-}M}$，$RN_{SP\text{-}M}$ 是否等于图6E的步骤208中的 $RN_{SP\text{-}M}$？
318
$RN_{SP\text{-}M}$ 是否正确？验证 AI_M 和 TA
否
320
拒绝消息
是
322
（1）SP分离 $DS_{EC\text{-}Private\text{-}Key}$，对 EC 的交易请求消息的数据部分执行散列算法：
$H(TID_{SP\text{-}EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC})=MD^{\wedge}_{EC}$
（2）SP 分离并得到：$TID_{SP\text{-}EC}$, $PLAIN\ TEXT_{EC}$, $CRYPTO_{EC}$, $DS_{EC\text{-}Private\text{-}Key}$
324
SP 使用 PK_{EC} 验证 $DS_{M\text{-}Private\text{-}Key}$，$MD^{\wedge}_{EC}$ 是否等于 MD_{EC}？（参见图5）
326
$MD^{\wedge}_{EC}$ 是否等于 MD_{EC}?
否
328
拒绝消息
是
330
$Skey_M$ 解密 $CRYPTO_{EC}$，恢复 $RN_{SP\text{-}EC}$，$RN_{SP\text{-}EC}$ 是否等于图6D的步骤184中的 $RN_{SP\text{-}EC}$？
332
$RN_{SP\text{-}EC}$ 是否正确？验证 AI_{EC} 和 TA
否
334
拒绝消息
是
KE阶段的终止
到图6L的步骤354
338
要发给 EC 的 SP 的响应数据
$Response\ Data_{SP\text{-}EC}$
336
SP 使用 $Skey_{EC}$ 加密：$E_{Skey\text{-}EC}(Response\ Data_{SP\text{-}EC})=CRYPTO_{SP\text{-}EC}$
SP 分配给 EC 的交易识别号：
$TID_{SP\text{-}EC}$（见步骤194）
342
要发给 EC 的 SP 的明文：
$PLAIN\ TEXT_{SP\text{-}EC}$
344
服务提供商组合：$TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}$
$*E_{Skey\text{-}EC}(Response\ Data_{SP\text{-}EC})=TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*CRYPTO_{SP\text{-}EC}$
340
到图6L的步骤346和352

图6L

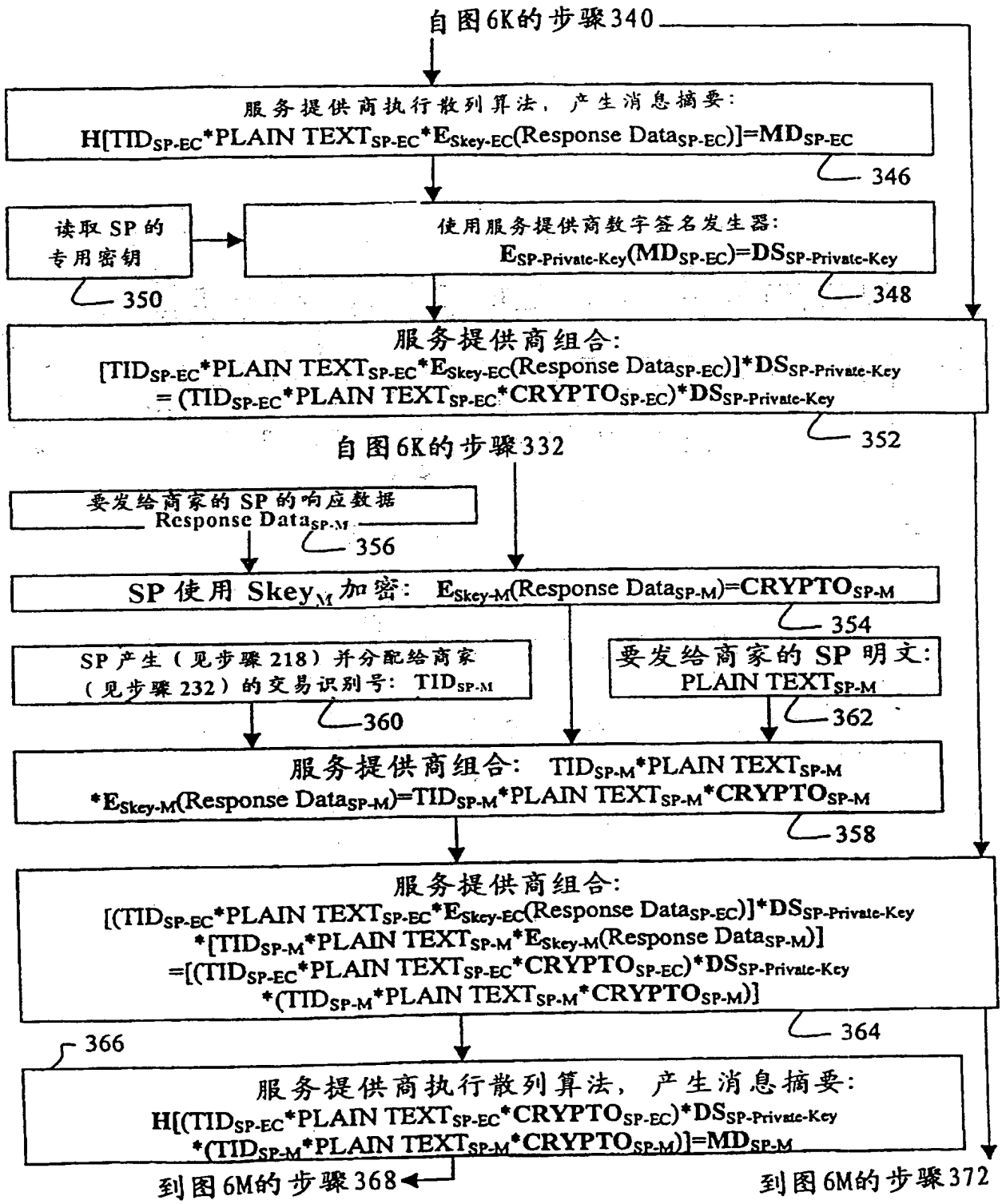

自图6K的步骤340
服务提供商执行散列算法，产生消息摘要：
H[TIDSP-EC*PLAIN TEXTSP-EC*ESkey-EC(Response DataSP-EC)]=MDSP-EC
346
读取SP的专用密钥
350
使用服务提供商数字签名发生器：
ESP-Private-Key(MDSP-EC)=DSSP-Private-Key
348
服务提供商组合：
[TIDSP-EC*PLAIN TEXTSP-EC*ESkey-EC(Response DataSP-EC)]*DSSP-Private-Key
=(TIDSP-EC*PLAIN TEXTSP-EC*CRYPTOSP-EC)*DSSP-Private-Key
352
自图6K的步骤332
要发给商家的SP的响应数据
Response DataSP-M
356
SP使用SkeyM加密：ESkey-M(Response DataSP-M)=CRYPTOSP-M
354
SP产生（见步骤218）并分配给商家（见步骤232）的交易识别号：TIDSP-M
360
要发给商家的SP明文：
PLAIN TEXTSP-M
362
服务提供商组合：TIDSP-M*PLAIN TEXTSP-M
*ESkey-M(Response DataSP-M)=TIDSP-M*PLAIN TEXTSP-M*CRYPTOSP-M
358
服务提供商组合：
[(TIDSP-EC*PLAIN TEXTSP-EC*ESkey-EC(Response DataSP-EC)]*DSSP-Private-Key
*[TIDSP-M*PLAIN TEXTSP-M*ESkey-M(Response DataSP-M)]
=[(TIDSP-EC*PLAIN TEXTSP-EC*CRYPTOSP-EC)*DSSP-Private-Key
*(TIDSP-M*PLAIN TEXTSP-M*CRYPTOSP-M)]
364
366
服务提供商执行散列算法，产生消息摘要：
H[(TIDSP-EC*PLAIN TEXTSP-EC*CRYPTOSP-EC)*DSSP-Private-Key
*(TIDSP-M*PLAIN TEXTSP-M*CRYPTOSP-M)]=MDSP-M
到图6M的步骤368
到图6M的步骤372

FIG. 6M

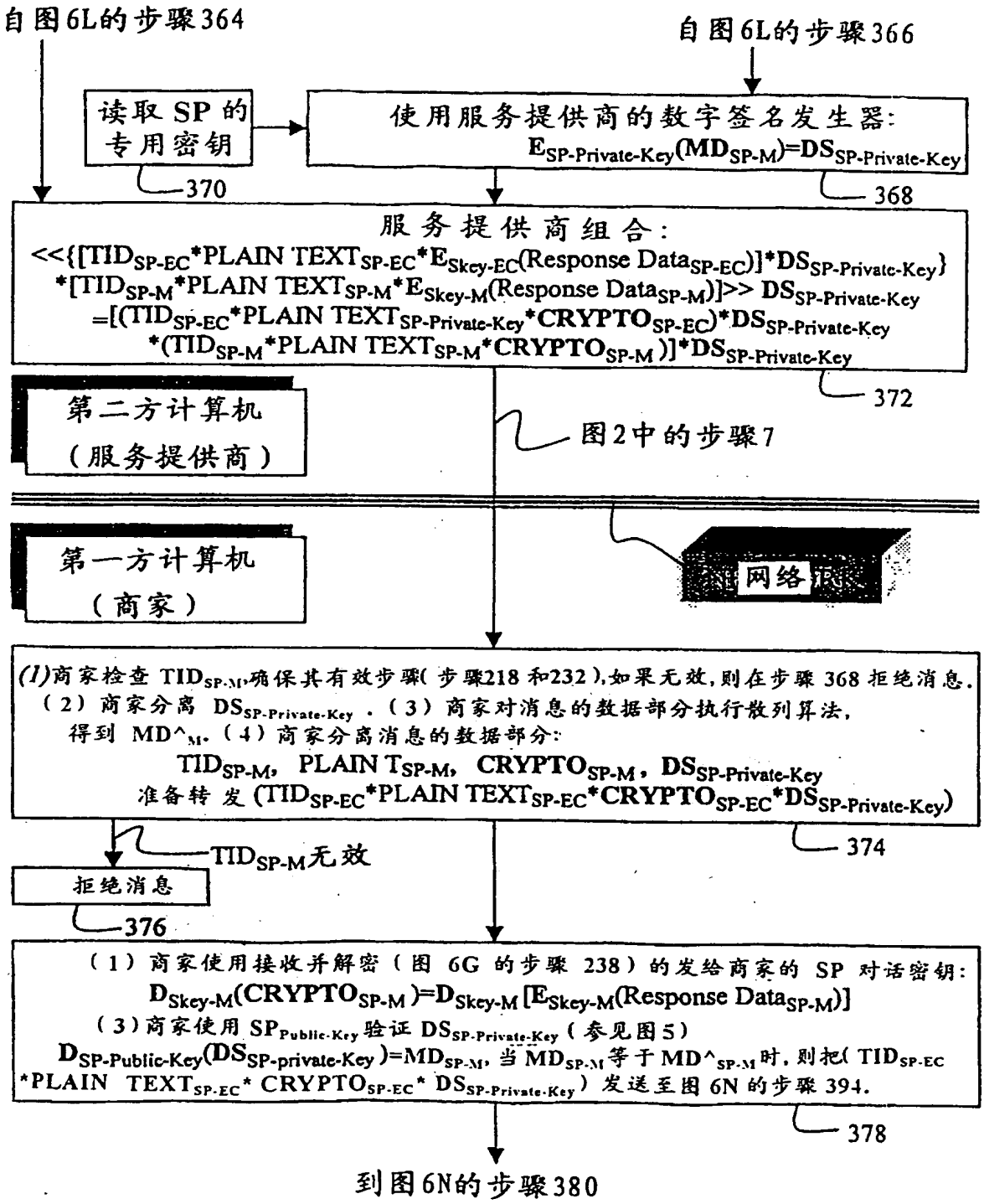

自图6L的步骤364
自图6L的步骤366
读取SP的专用密钥
370
使用服务提供商的数字签名发生器:
$E_{SP\text{-}Private\text{-}Key}(MD_{SP\text{-}M})=DS_{SP\text{-}Private\text{-}Key}$
368
服务提供商组合:
$<<\{[TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*E_{Skey\text{-}EC}(Response\ Data_{SP\text{-}EC})]*DS_{SP\text{-}Private\text{-}Key}\}$
$*[TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*E_{Skey\text{-}M}(Response\ Data_{SP\text{-}M})]>>DS_{SP\text{-}Private\text{-}Key}$
$=[(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}Private\text{-}Key}*CRYPTO_{SP\text{-}EC})*DS_{SP\text{-}Private\text{-}Key}$
$*(TID_{SP\text{-}M}*PLAIN\ TEXT_{SP\text{-}M}*CRYPTO_{SP\text{-}M})]*DS_{SP\text{-}Private\text{-}Key}$
372
第二方计算机
(服务提供商)
图2中的步骤7
第一方计算机
(商家)
网络
(1)商家检查 $TID_{SP\text{-}M}$,确保其有效步骤(步骤218和232),如果无效,则在步骤368拒绝消息.
(2)商家分离 $DS_{SP\text{-}Private\text{-}Key}$.(3)商家对消息的数据部分执行散列算法,
得到 $MD^{\wedge}_{M}$.(4)商家分离消息的数据部分:
$TID_{SP\text{-}M}$, PLAIN $T_{SP\text{-}M}$, $CRYPTO_{SP\text{-}M}$, $DS_{SP\text{-}Private\text{-}Key}$
准备转发 $(TID_{SP\text{-}EC}*PLAIN\ TEXT_{SP\text{-}EC}*CRYPTO_{SP\text{-}EC}*DS_{SP\text{-}Private\text{-}Key})$
374
$TID_{SP\text{-}M}$无效
拒绝消息
376
(1)商家使用接收并解密(图6G的步骤238)的发给商家的SP对话密钥:
$D_{Skey\text{-}M}(CRYPTO_{SP\text{-}M})=D_{Skey\text{-}M}[E_{Skey\text{-}M}(Response\ Data_{SP\text{-}M})]$
(3)商家使用 $SP_{Public\text{-}Key}$ 验证 $DS_{SP\text{-}Private\text{-}Key}$(参见图5)
$D_{SP\text{-}Public\text{-}Key}(DS_{SP\text{-}private\text{-}Key})=MD_{SP\text{-}M}$,当 $MD_{SP\text{-}M}$ 等于 $MD^{\wedge}_{SP\text{-}M}$ 时,则把($TID_{SP\text{-}EC}$
$*PLAIN\ TEXT_{SP\text{-}EC}*\ CRYPTO_{SP\text{-}EC}*\ DS_{SP\text{-}Private\text{-}Key}$)发送至图6N的步骤394.
378
到图6N的步骤380

图6N

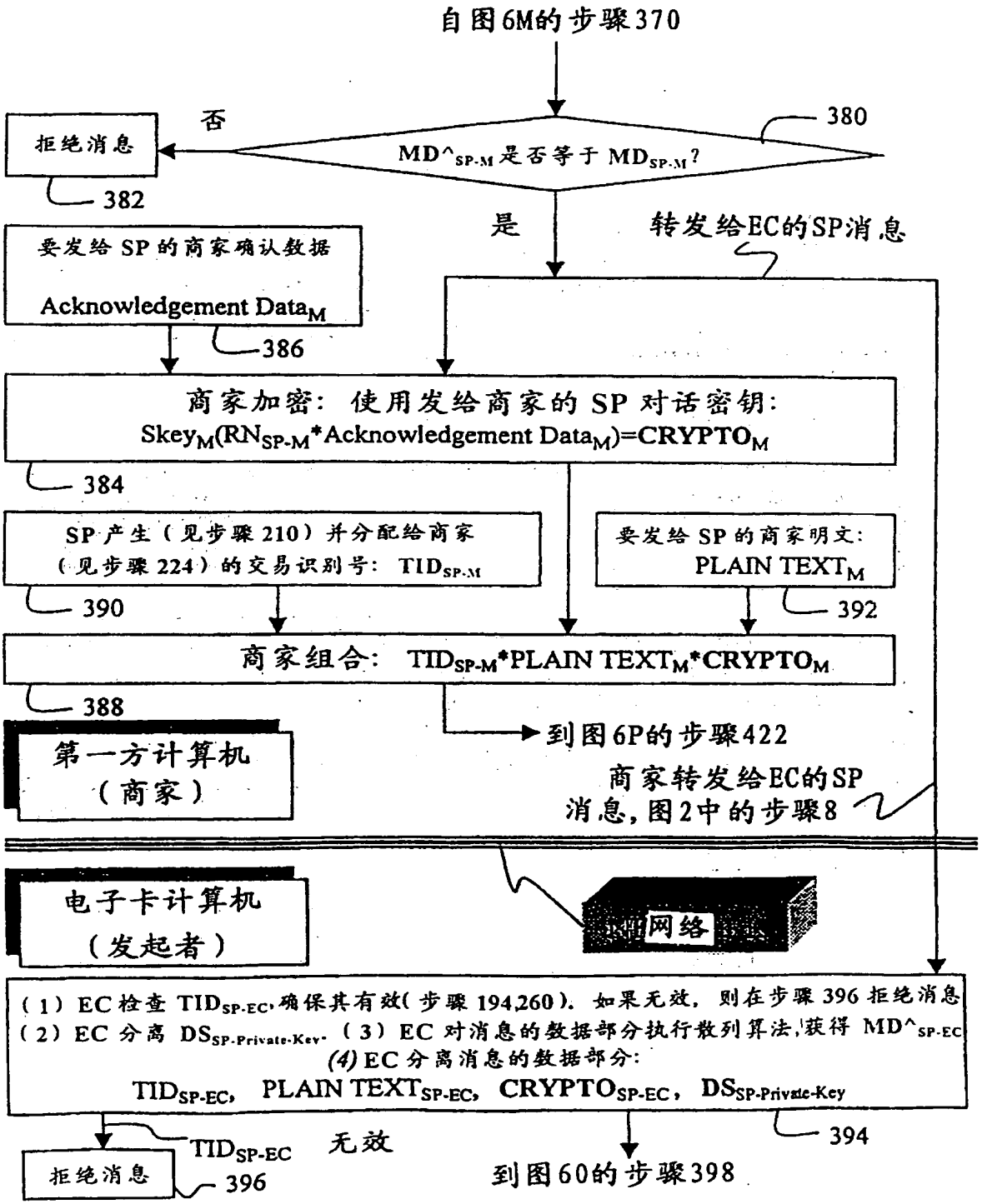

自图6M的步骤370
否
拒绝消息
382
MD^SP-M是否等于MDSP-M?
380
是
转发给EC的SP消息
要发给SP的商家确认数据
AcknowledgementDataM
386
商家加密：使用发给商家的SP对话密钥：
SkeyM(RNSP-M*AcknowledgementDataM)=CRYPTOM
384
SP产生（见步骤210）并分配给商家（见步骤224）的交易识别号：TIDSP-M
390
要发给SP的商家明文：
PLAIN TEXTM
392
商家组合：TIDSP-M*PLAIN TEXTM*CRYPTOM
388
到图6P的步骤422
第一方计算机（商家）
商家转发给EC的SP消息，图2中的步骤8
电子卡计算机（发起者）
网络
（1）EC检查TIDSP-EC，确保其有效（步骤194,260）。如果无效，则在步骤396拒绝消息
（2）EC分离DSSP-Private-Key。（3）EC对消息的数据部分执行散列算法，获得MD^SP-EC
(4) EC分离消息的数据部分：
TIDSP-EC, PLAIN TEXTSP-EC, CRYPTOSP-EC, DSSP-Private-Key
394
TIDSP-EC 无效
拒绝消息
396
到图60的步骤398

图6O

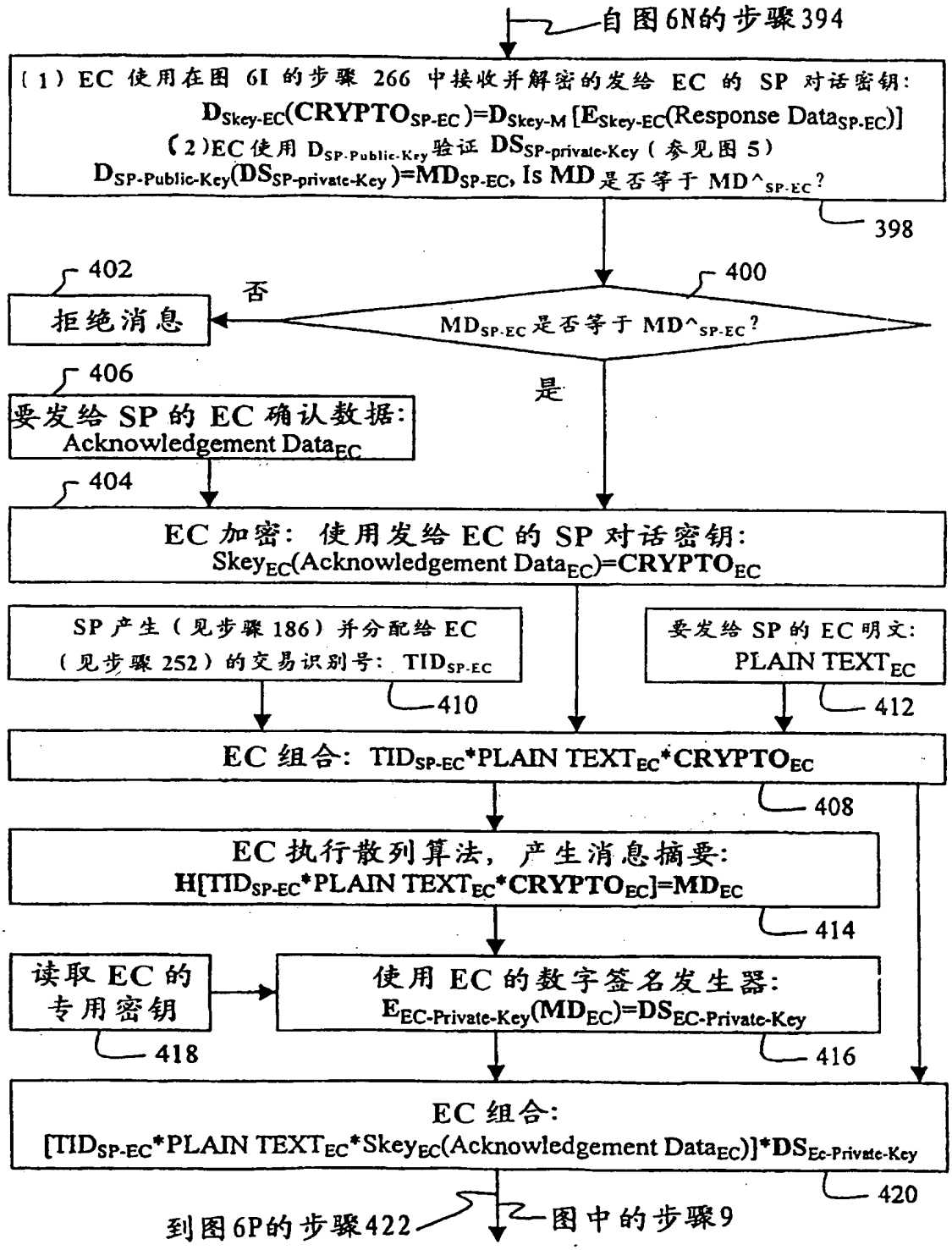

自图6N的步骤394
(1) EC 使用在图 6I 的步骤 266 中接收并解密的发给 EC 的 SP 对话密钥:
$D_{Skey-EC}(CRYPTO_{SP-EC})=D_{Skey-M}[E_{Skey-EC}(Response\ Data_{SP-EC})]$
(2)EC 使用 $D_{SP-Public-Key}$ 验证 $DS_{SP-private-Key}$ (参见图 5)
$D_{SP-Public-Key}(DS_{SP-private-Key})=MD_{SP-EC}$, Is MD 是否等于 MD^$_{SP-EC}$?
398
402
拒绝消息
否
400
MD_{SP-EC} 是否等于 MD^$_{SP-EC}$?
是
406
要发给 SP 的 EC 确认数据:
Acknowledgement $Data_{EC}$
404
EC 加密: 使用发给 EC 的 SP 对话密钥:
$Skey_{EC}(Acknowledgement\ Data_{EC})=CRYPTO_{EC}$
SP 产生 (见步骤 186) 并分配给 EC (见步骤 252) 的交易识别号: TID_{SP-EC}
410
要发给 SP 的 EC 明文:
$PLAIN\ TEXT_{EC}$
412
EC 组合: TID_{SP-EC}*$PLAIN\ TEXT_{EC}$*$CRYPTO_{EC}$
408
EC 执行散列算法, 产生消息摘要:
$H[TID_{SP-EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC}]=MD_{EC}$
414
读取 EC 的专用密钥
418
使用 EC 的数字签名发生器:
$E_{EC-Private-Key}(MD_{EC})=DS_{EC-Private-Key}$
416
EC 组合:
$[TID_{SP-EC}*PLAIN\ TEXT_{EC}*Skey_{EC}(Acknowledgement\ Data_{EC})]*DS_{Ec-Private-Key}$
420
到图6P的步骤422
图中的步骤9

图6P

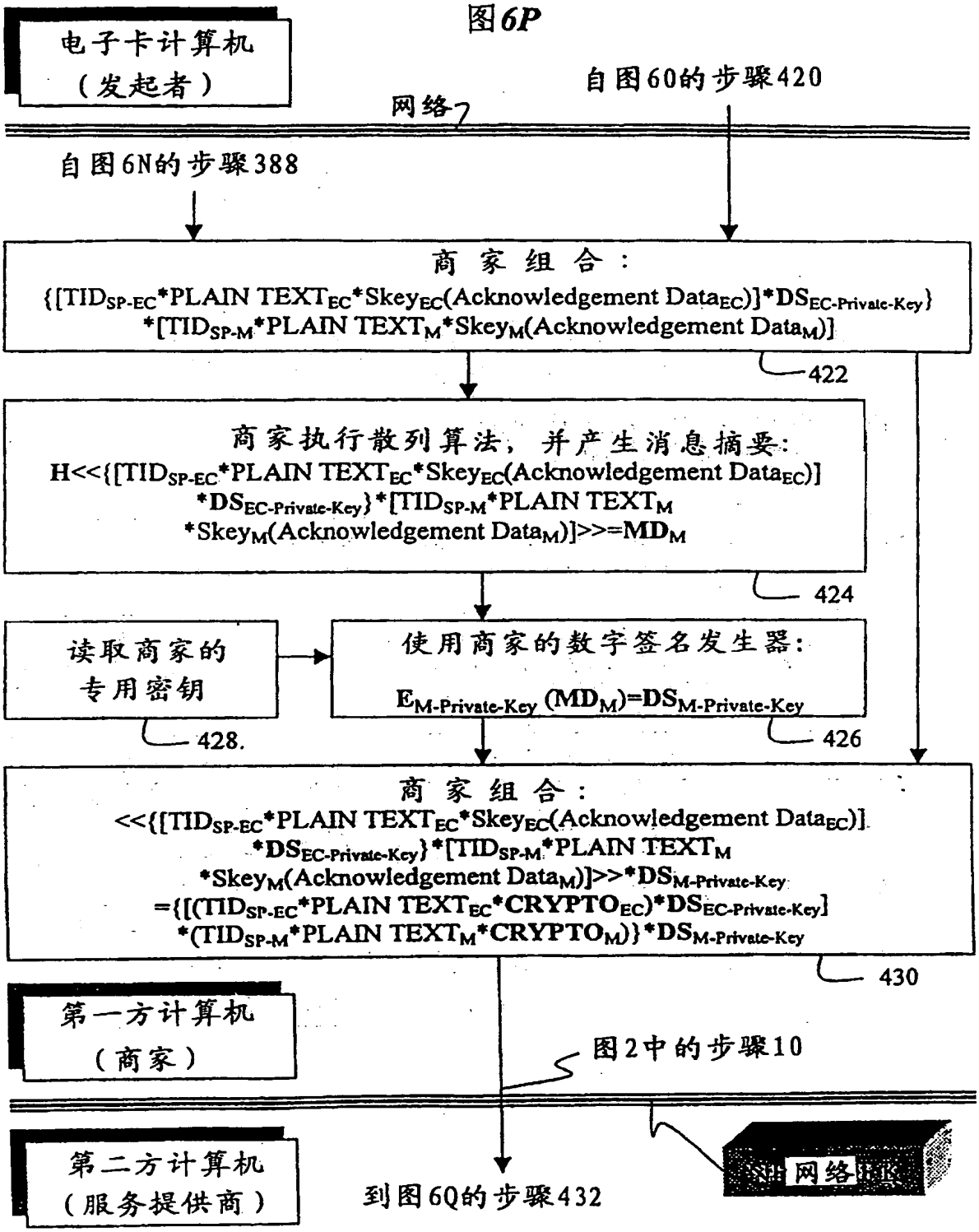

电子卡计算机
（发起者）
网络7
自图60的步骤420
自图6N的步骤388
商家组合：
{[TIDSP-EC*PLAIN TEXTEC*SkeyEC(Acknowledgement DataEC)]*DSEC-Private-Key}
*[TIDSP-M*PLAIN TEXTM*SkeyM(Acknowledgement DataM)]
422
商家执行散列算法，并产生消息摘要：
H<<{[TIDSP-EC*PLAIN TEXTEC*SkeyEC(Acknowledgement DataEC)]
DSEC-Private-Key}[TIDSP-M*PLAIN TEXTM
*SkeyM(Acknowledgement DataM)]>>=MDM
424
读取商家的
专用密钥
428.
使用商家的数字签名发生器：
EM-Private-Key (MDM)=DSM-Private-Key
426
商家组合：
<<{[TIDSP-EC*PLAIN TEXTEC*SkeyEC(Acknowledgement DataEC)]
DSEC-Private-Key}[TIDSP-M*PLAIN TEXTM
*SkeyM(Acknowledgement DataM)]>>*DSM-Private-Key
={[(TIDSP-EC*PLAIN TEXTEC*CRYPTOEC)*DSEC-Private-Key]
*(TIDSP-M*PLAIN TEXTM*CRYPTOM)}*DSM-Private-Key
430
第一方计算机
（商家）
图2中的步骤10
第二方计算机
（服务提供商）
到图6Q的步骤432
网络

图6Q

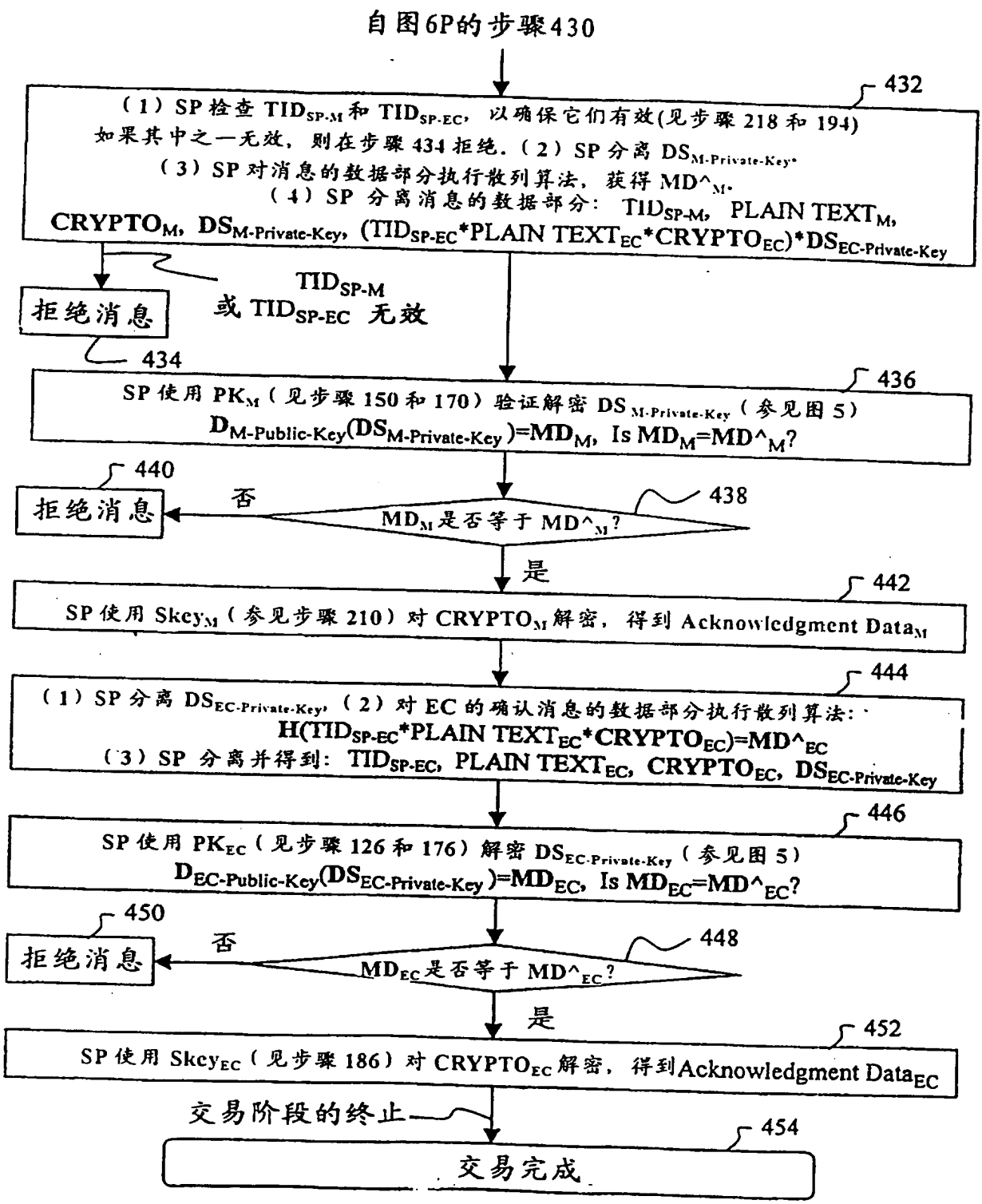

自图6P的步骤430
(1) SP检查 TID_{SP-M}和 TID_{SP-EC}，以确保它们有效(见步骤218和194)
如果其中之一无效，则在步骤434拒绝。(2) SP分离 $DS_{M-Private-Key}$。
(3) SP对消息的数据部分执行散列算法，获得 $MD^{\wedge}_{M}$。
(4) SP分离消息的数据部分：TID_{SP-M}，PLAIN $TEXT_{M}$，
$CRYPTO_{M}$，$DS_{M-Private-Key}$，$(TID_{SP-EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC})*DS_{EC-Private-Key}$
432
拒绝消息
TID_{SP-M}
或 TID_{SP-EC} 无效
434
SP使用 PK_{M}（见步骤150和170）验证解密 $DS_{M-Private-Key}$（参见图5）
$D_{M-Public-Key}(DS_{M-Private-Key})=MD_{M}$，Is $MD_{M}=MD^{\wedge}_{M}$?
436
440
拒绝消息
否
MD_{M}是否等于 $MD^{\wedge}_{M}$?
438
是
SP使用 $Skey_{M}$（参见步骤210）对 $CRYPTO_{M}$解密，得到 Acknowledgment $Data_{M}$
442
(1) SP分离 $DS_{EC-Private-Key}$，(2) 对EC的确认消息的数据部分执行散列算法：
$H(TID_{SP-EC}*PLAIN\ TEXT_{EC}*CRYPTO_{EC})=MD^{\wedge}_{EC}$
(3) SP分离并得到：TID_{SP-EC}，PLAIN $TEXT_{EC}$，$CRYPTO_{EC}$，$DS_{EC-Private-Key}$
444
SP使用 PK_{EC}（见步骤126和176）解密 $DS_{EC-Private-Key}$（参见图5）
$D_{EC-Public-Key}(DS_{EC-Private-Key})=MD_{EC}$，Is $MD_{EC}=MD^{\wedge}_{EC}$?
446
450
拒绝消息
否
MD_{EC}是否等于 $MD^{\wedge}_{EC}$?
448
是
SP使用 $Skey_{EC}$（见步骤186）对 $CRYPTO_{EC}$解密，得到Acknowledgment $Data_{EC}$
452
交易阶段的终止
454
交易完成

图7

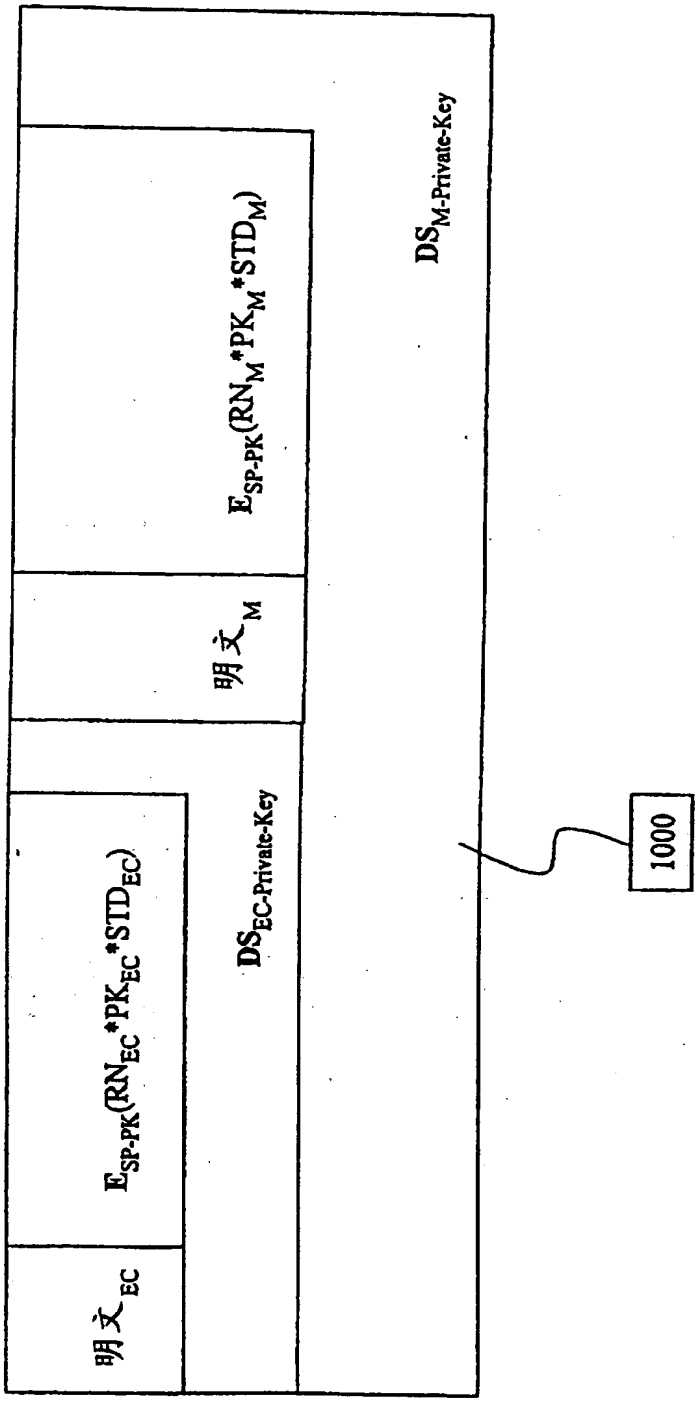

明文EC
ESP-PK(RNEC*PKEC*STDEC)
DSEC-Private-Key
明文M
ESP-PK(RNM*PKM*STDM)
DSM-Private-Key
1000

图8

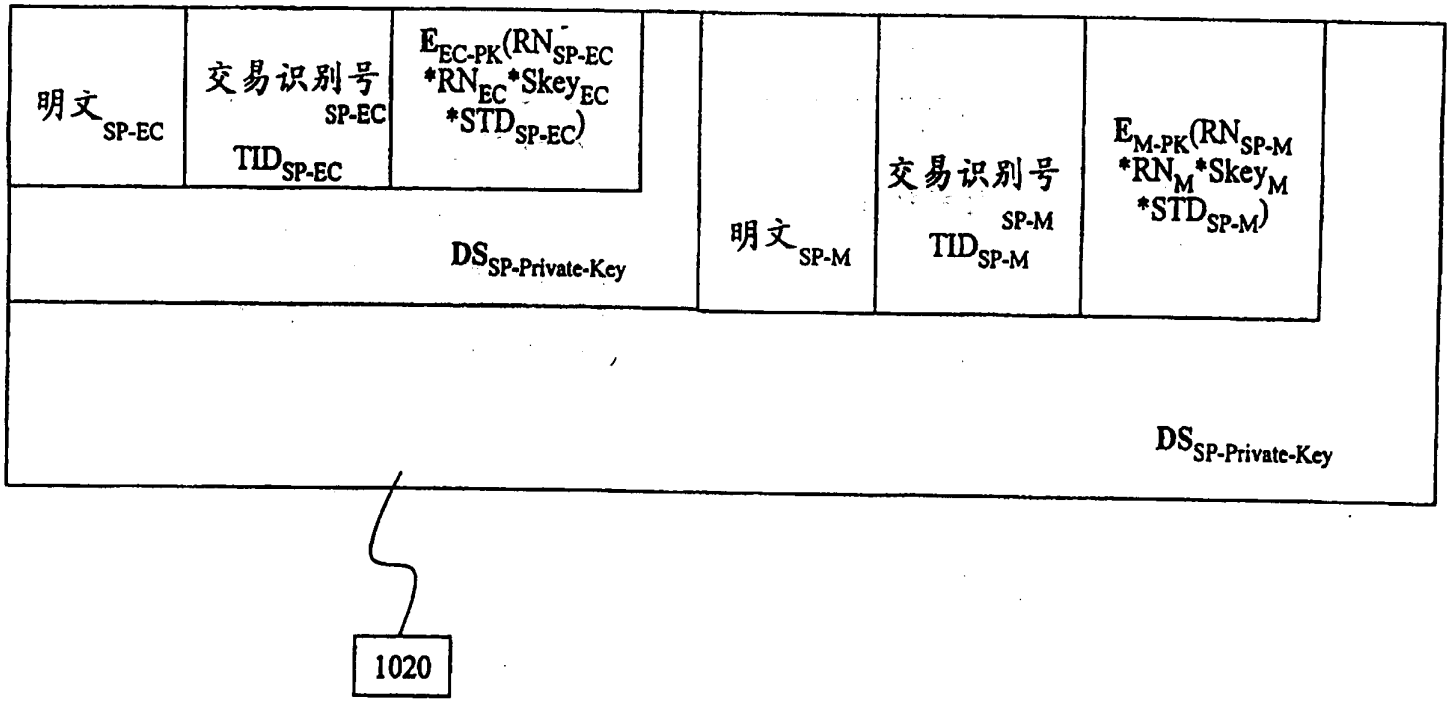

明文SP-EC
交易识别号SP-EC
TIDSP-EC
EEC-PK(RNSP-EC *RNEC*SkeyEC *STDSP-EC)
DSSP-Private-Key
明文SP-M
交易识别号SP-M
TIDSP-M
EM-PK(RNSP-M *RNM*SkeyM *STDSP-M)
DSSP-Private-Key
1020

图9

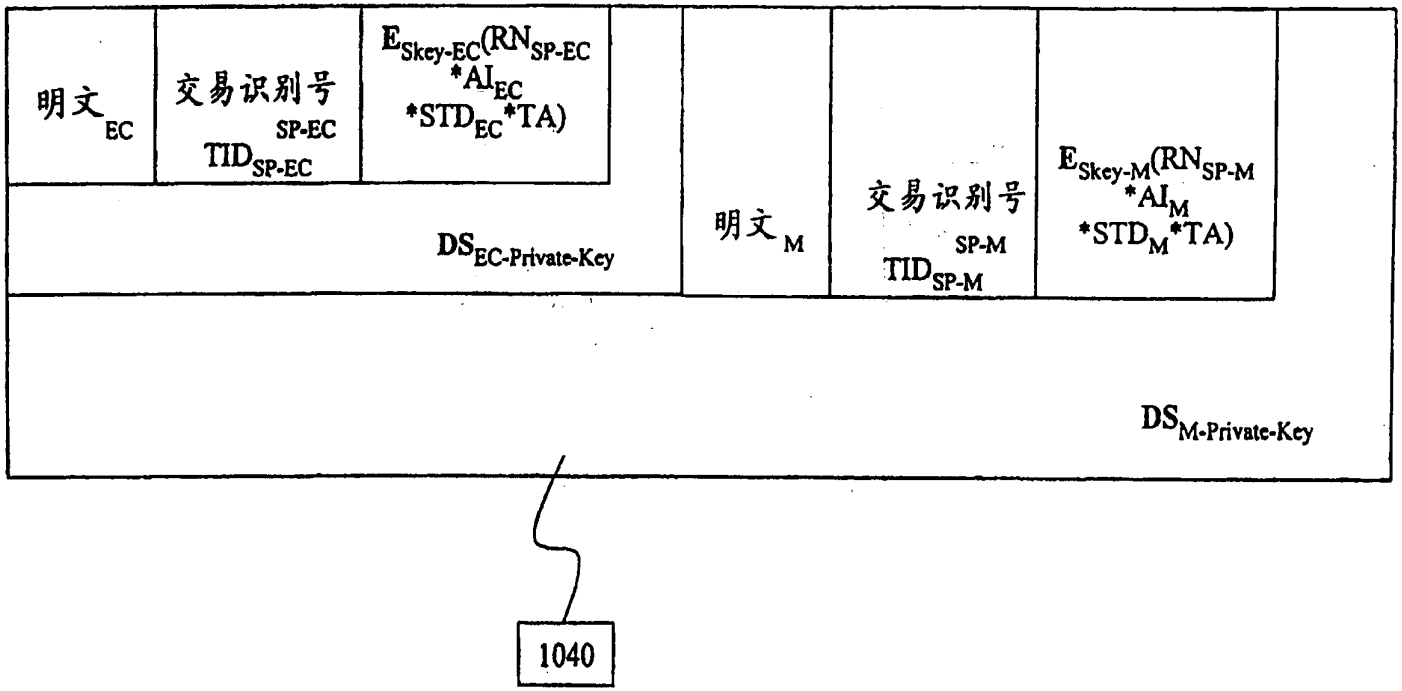

明文EC
交易识别号SP-EC TIDSP-EC
ESkey-EC(RNSP-EC *AIEC *STDEC*TA)
DSEC-Private-Key
明文M
交易识别号SP-M TIDSP-M
ESkey-M(RNSP-M *AIM *STDM*TA)
DSM-Private-Key
1040

图10

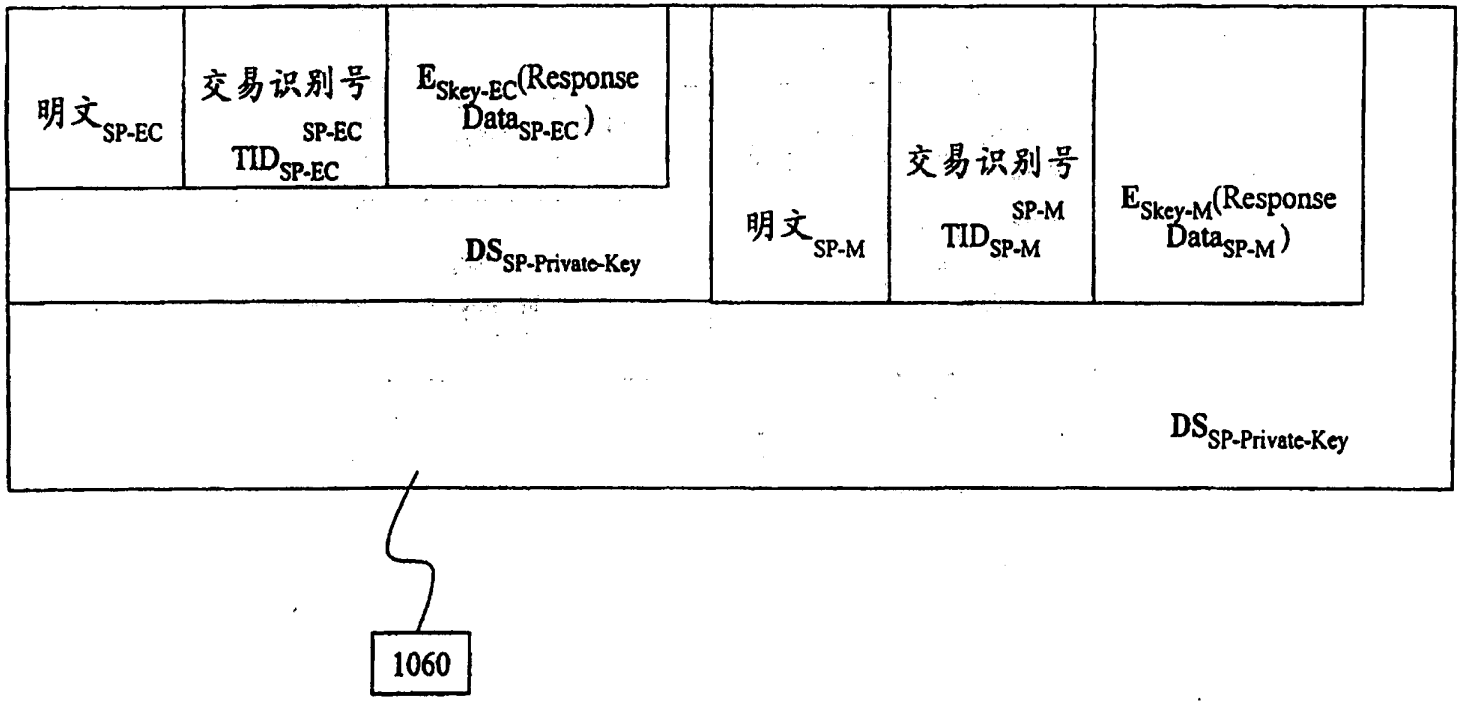

明文SP-EC
交易识别号 SP-EC TIDSP-EC
ESkey-EC(Response DataSP-EC)
DSSP-Private-Key
明文SP-M
交易识别号 SP-M TIDSP-M
ESkey-M(Response DataSP-M)
DSSP-Private-Key
1060

图11

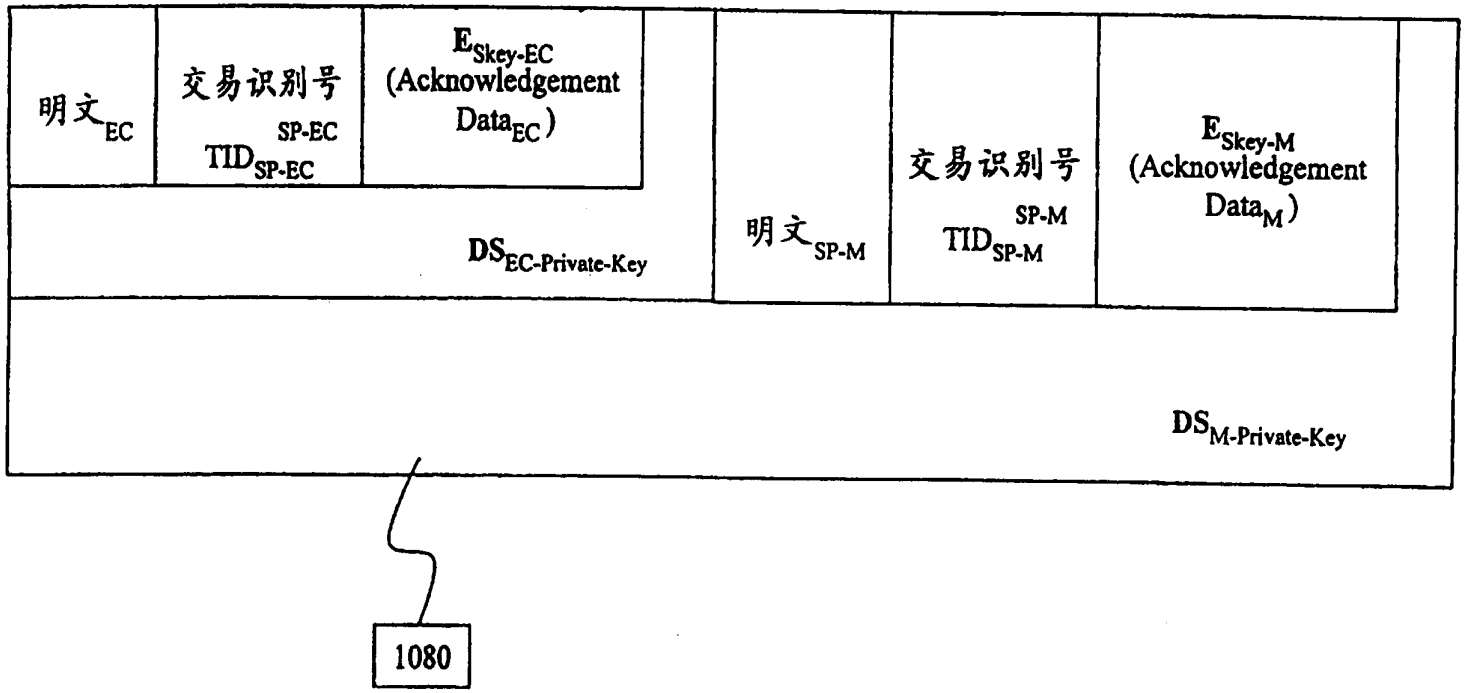

明文EC
交易识别号 SP-EC TIDSP-EC
ESkey-EC (Acknowledgement DataEC)
DSEC-Private-Key
明文SP-M
交易识别号 SP-M TIDSP-M
ESkey-M (Acknowledgement DataM)
DSM-Private-Key
1080

图12

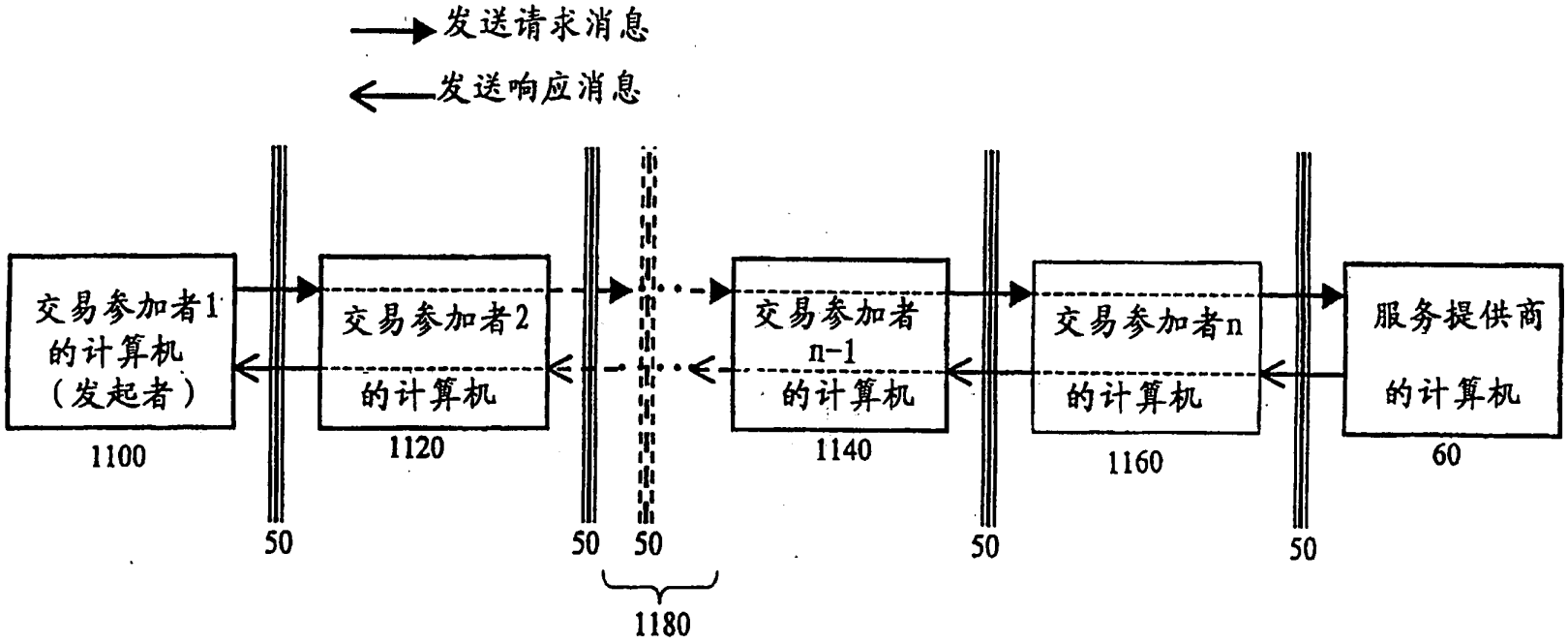
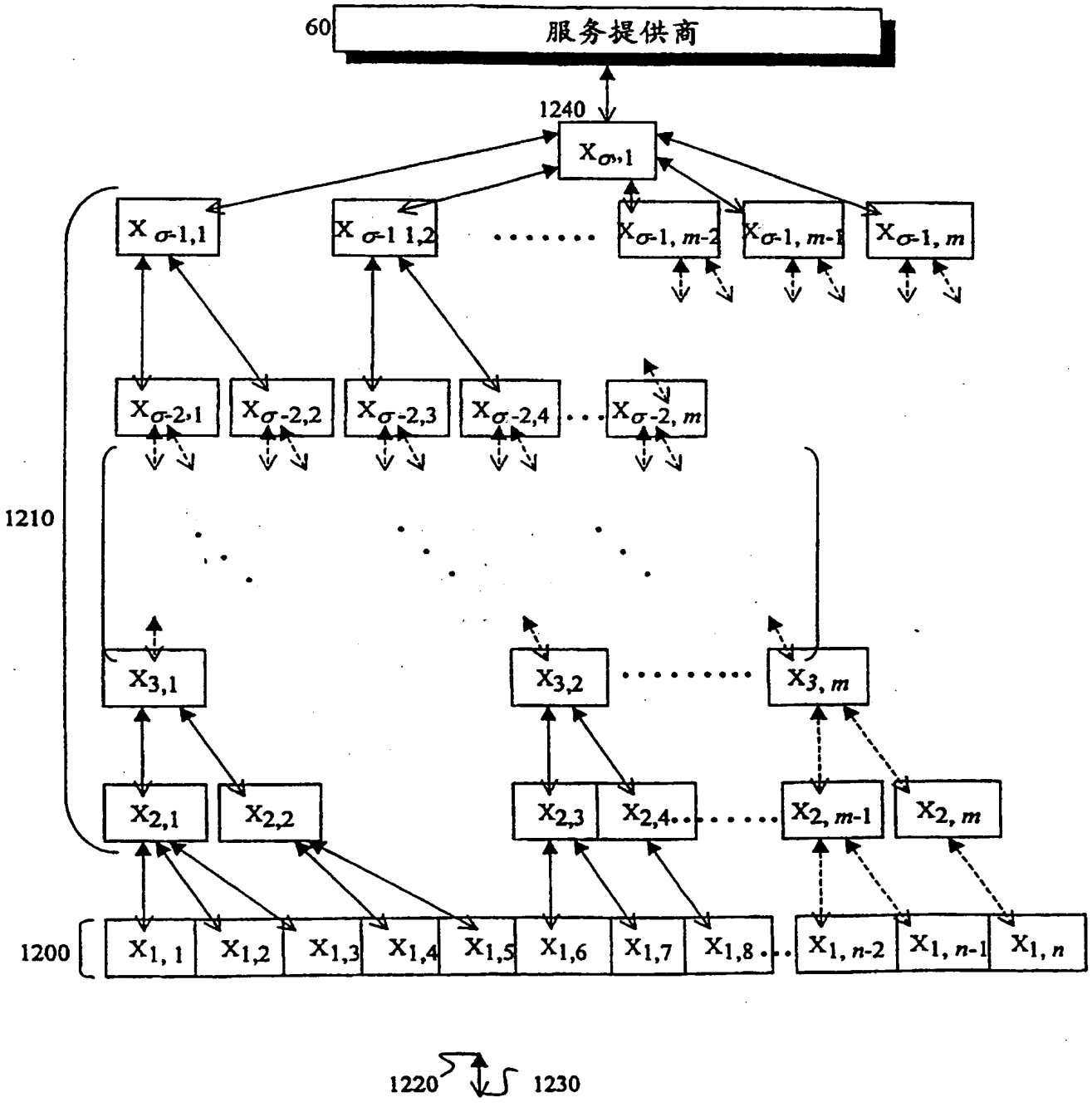

发送请求消息
发送响应消息
交易参加者1的计算机（发起者）
1100
交易参加者2的计算机
1120
交易参加者n-1的计算机
1140
交易参加者n的计算机
1160
服务提供商的计算机
60
50
50
50
50
50
1180

图13


60
服务提供商
1240
$X_{\sigma,1}$
$X_{\sigma-1,1}$
$X_{\sigma-1,2}$
$X_{\sigma-1,m-2}$
$X_{\sigma-1,m-1}$
$X_{\sigma-1,m}$
$X_{\sigma-2,1}$
$X_{\sigma-2,2}$
$X_{\sigma-2,3}$
$X_{\sigma-2,4}$
$X_{\sigma-2,m}$
1210
$X_{3,1}$
$X_{3,2}$
$X_{3,m}$
$X_{2,1}$
$X_{2,2}$
$X_{2,3}$
$X_{2,4}$
$X_{2,m-1}$
$X_{2,m}$
1200
$X_{1,1}$
$X_{1,2}$
$X_{1,3}$
$X_{1,4}$
$X_{1,5}$
$X_{1,6}$
$X_{1,7}$
$X_{1,8}$
$X_{1,n-2}$
$X_{1,n-1}$
$X_{1,n}$
1220
1230